UNIVERSITY OF Southampton

Faculty of Engineering and Physical Sciences

School of Electronics and Computer Science

Web and Internet Science

Analysing the impact of the GDPR on eIDAS:

Supporting effective Data Protection by Design for cross-border electronic identification through unlinkability measures

by

Niko Tsakalakis

https://orcid.org/0000-0003-2654-0825

Thesis for the degree of Doctor of Philosophy

November 2020

University of Southampton

Abstract

Faculty of Engineering and Physical Sciences
School of Electronics and Computer Science
Web and Internet Science

Doctor of Philosophy

Analysing the impact of the GDPR on eIDAS: Supporting effective Data Protection by Design for cross-border electronic identification through unlinkability measures

by Niko Tsakalakis

The European Commission has decided to accelerate the use of electronic identification for digital services between Member States through the adoption of the Regulation on electronic identification and trust services, 'eIDAS'. eIDAS aims at establishing the mutual recognition of national eID schemes whilst offering strong confidentiality, security and protection of personal data. In the meantime, EU's data protection regime has been updated under the EU General Data Protection Regulation, the 'GDPR', which introduced an obligation of 'data protection by design' and made explicit a risk-based approach to the protection of personal data.

This research explores the interplay between eIDAS and the GDPR. For the interoperability of electronic identification services, eIDAS sets up an Interoperability Framework which comprises technical requirements, required attributes representing a natural or legal person, procedural rules, dispute resolution arrangements, and common security standards. The research findings enable the assessment of the degree that the Interoperability Framework is 'fit-for-purpose' for a high level of 'by design' protection on intra-EU flows of personal data.

A mixed methods triangulation-based approach is used to determine the adequacy of the level of data protection afforded by eIDAS' Interoperability Framework. Desk research is employed to clarify the substance of data protection by design. A data protection by design methodology is proposed based on risk assessment and it is then used to assess the current specifications of eIDAS. Three case studies of national electronic identification services are analysed in order to elicit the state of the art in terms of data protection by design. The findings are then evaluated through interviews with experts in the field of electronic identification.

This thesis argues that the definition of a mandatory set of person identification data, among which a persistent unique identifier, in the current implementation of the Interoperability Framework overlooks the importance of unlinkability and addresses the principles of data minimisation and purpose limitation insufficiently. Further, it asserts that the existence of the mandatory set hampers the effective use of pseudonymisation and will in certain cases lower the level of data protection guaranteed by some Member States.

The thesis concludes that lowering the level of data protection would be hard to justify against the contextual factors of data protection by design, i.e. the state of the art, the cost of implementation and the risks posed to the individuals. It suggests a practical solution to increase the level of data protection by implementing pseudonymisation and selective disclosure functionality in the eIDAS-nodes that mediate the communication of the national services. This thesis, therefore, provides contributions that help to understand the newly introduced notion of data protection by design, proposes a way to contextualise its implications for cross-border electronic identification, and offers a way to strengthen unlinkability in the Interoperability Framework.

Declaration of Authorship

I, Niko Tsakalakis , declare that the thesis entitled *Analysing the impact of the GDPR on eIDAS: Supporting effective Data Protection by Design for cross-border electronic identification through unlinkability measures* and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as indicated in the **List of publications**.

Signed: ....

Date: ....

List of publications

Peer reviewed papers

- Niko Tsakalakis, Kieron O'Hara, and Sophie Stalla-Bourdillon, *"Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation"* (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), 21 May 2016, Hannover, Germany, 2016) DOI: 10.1145/2908131.2908152
- Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation"* (Detlef Hühnlein and others eds, Open Identity Summit, 15 September 2016, Rome, Italy, 2016) vol P-264 ⟨https://dl.gi.de/handle/20.500.12116/598⟩ accessed 12 January 2019
- Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (2017) 3(3) The Journal of Web Science 32 DOI: 10.1561/106.00000010
- Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17

Contributions to the EU project 'FutureTrust'

- Niko Tsakalakis, Sophie Stalla-Bourdillon, and Marc Sel, *Deliverable 2.7: State of the art in relation to privacy and data protection requirements: Preliminary report* (Ref. Ares(2017)522263 - 31/01/2017, FutureTrust consortium 2017) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_ca38279654cc476fb24ecf5657b8be71.pdf⟩ accessed 25 May 2019 (archived at ⟨https://tinyurl.com/ujsvcwm⟩)
- Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩)
- Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 5.3: Legal evaluation of the FutureTrust architecture* (Ref. Ares(2019)4856595 - 25/07/2019, FutureTrust consortium 2019) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_6ee720db94a444b98f1cadafeefca1db.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/ycnogogd⟩)

Acknowledgements

I would like to express my deepest gratitude to my supervisors, Dr Kieron O’Hara and Professor Sophie Stalla-Bourdillon, for their incredible help and support over the course of my PhD. I am deeply indebted to Sophie in particular, who has offered invaluable advice, guidance and feedback at every stage towards the production of this thesis and has actively encouraged my professional development for the past 5 years. This thesis would not have been possible without her support. Similarly, I must also thank the lecturers and professors within WAIS, ECS and the social sciences, who have offered their extensive knowledge and insightful suggestions over these years. I would like to extend a special thanks to Professor Les Carr, who was partly responsible for my acceptance into the PhD programme and has been a supporting figure to all of us ‘Web Scientists’ throughout, and Professor Susan Halford who never backed down from a debate and was there to challenge my assumptions when I needed it the most.

To my fellow Web Science cohort, I cannot thank you enough for your help, support and friendship. I should also thank the Web Science Doctoral Training Centre, which provided me with the opportunity to carry out this research, and especially to all of the staff who have continuously offered fantastic opportunities for growth but most importantly have recognised, encouraged and celebrated the contribution that each one of us brought to the DTC.

I cannot begin to express my thanks to Briony, Sarah and Nick who have been alongside me in this adventure and made me feel welcome and appreciated – you are a constant reminder of the things I love most about this country. I must also thank my Greeks and adopted Greeks, Αλκυόνη, Βασίλη x2, Βάσω, Έλενα, Ερατώ, Μαρία, Παναγιώτη and Thomas, as well as all the friends back home, who have endured me throughout all this and never wavered in their support.

Finally, I would not have seen this through without Peny, who agreed to share a house 6 years ago only to become my family ever since. Πένυ, I will never be able to put into words how much I appreciate it. Finally, a big thanks to my mum and my sis who may consider PhDs as compulsory education but without whom I wouldn’t be ‘me’.

Mum, we did it!

Contents

List of Cases

Table of EU Cases (Alphabetical)

Table of EU Cases (Numerical)

Table of International Cases

Table of Cases from National Jurisdictions

List of Legislation

Table of International Treaties

Table of EU Treaties

Table of EU Legislation

Table of National Legislation

List of Figures

List of Tables

List of Listings

List of Abbreviations

General Abbreviations

BSI	Federal Office for Information Security (Germany).
CRR	Central Residents Register (Austria).
DPA	Data Protection Authority.
DPIA	Data Protection Impact Assessment.
DPO	Data Protection Officer.
EDPB	European Data Protection Board; *see also* WP29.
EEA	European Economic Area.
EU	European Union.
GDS	Government Digital Service (UK).
ICT	Information and Communication Technology.
PIA	Privacy Impact Assessment; *see also* DPIA.
SDM	Standard Data Protection Model (DPIA framework).
WP29	Article 29 Data Protection Working Party; *see also* EDPB.

eID Related

eID	Electronic Identification; *Glossary:* Electronic identification (eID).

nPA	Neuer Personalausweiss eID scheme (Germany).
ACC	Austrian Citizen Card eID scheme (Austria).
IdP	Identity Provider.
LoA	Level Of Assurance.
PID	Persistent Identifier; *Glossary:* unique identifier.
SAML	Security Assertion Markup Language.
SOAP	Simple Object Access Protocol.
sPIN	source Personal Identification Number.
ssPIN	sector-specific Personal Identification Number.
SSO	Single Sign-on.

Legislation Related

eIDAS	Regulation (EU) No 910/2014 on Electronic Identification And Trust Services.
CJEU	The Court Of Justice Of The European Union.
GDPR	General Data Protection Regulation.
RTS	Regulatory Technical Standard.

List of Terms

This thesis uses the terminology as defined in *Common Terminological Framework for Interoperable Electronic Identity Management*.[1] Where the term also appears in eIDAS,[2] its definition is also noted, prepended with [eIDAS:].

A

`Anonymity`

The quality or state of being not identifiable within the set of all possible entities that could cause an action and that might be addressed.

`Assertion`

Assertion is synonymous with a credential.

`Attribute`

A distinct, measurable, physical or abstract named property belonging to an entity.

`Authentication`

The corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence
[eIDAS:] *an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed*

[1] Modinis IDM Study Team (ed), *Common Terminological Framework for Interoperable Electronic Identity Management* (techspace rep, 2.01, Europäische Gemeinschaft - eGovernment Unit 2005) ⟨https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf⟩ accessed 17 January 2020 (archived at ⟨https://tinyurl.com/yxyt942w⟩).

[2] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

`Authentication token`

Any hardware or software that contains credentials related to attributes used for authentication purposes.

`C`

`Corroboration`

The confirmation by provision of sufficient evidence and examination thereof that specified requirements have been fulfilled.

`Credential`

A piece of information attesting to the integrity of certain stated facts.

`E`

`eID means`

A material and/or immaterial unit containing person identification data and which is used for authentication for an online service; *see* eID token.

`eID scheme`

A system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.

`eID token`

Any hardware or software that contains credentials related to attributes; *see also* authentication token, eID means.

`Electronic identification (eID)`

The process of using claimed or observed attributes of an entity to deduce who the entity is

[eIDAS:] *the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person*

`Enrolment`

Synonymous with a registration.

`Entity`

Anyone (natural or legal person) or anything that shall be characterised through the measurement of its attributes.

Entity authentication

The corroboration of the claimed identity of an entity and a set of its observed attributes; *see also* authentication.

F

Federated identity

A credential of an entity that links an entity's partial identity from one context to a partial identity from another context.

I

Identifier

An attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context; *see also* unique identifier.

P

Person identification data

A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established; *see* attribute.

Privacy enhancing technology

Hardware or software which increases the ability of a natural person to actively influence the availability of information about and exposure of itself.

Pseudonym

An arbitrary identifier of an identifiable entity, by which a certain action can be linked to this specific entity. The entity that may be identified by the pseudonym is the holder of the pseudonym.

R

Registration

The process in which the entity is identified and/or other attributes are corroborated. As a result of the registration, a partial identity is assigned to the entity for a certain context.

Relying party

A natural or legal person that relies upon an electronic identification or a trust service.

U

Unique identifier

An identifier such as a unique number or any set of attributes that allows one to determine precisely who or what the entity is; *see also* identifier.

V

Verification

A synonym of corroboration.

God bless the book people for their boundless knowledge,
absorbed from having words instead of friends

— Mackenzi Lee, The Gentleman's Guide to Vice and Virtue

Chapter 1

Introduction

In its 2010 *"Digital Agenda for Europe"*, the European Commission recognised the *"key enabling role"*[3] that the Internet shall play in exiting the economic crisis of 2008 and preparing the European Union (EU) economy for the challenges of the future. The use of Information and Communication Technology (ICT) to deliver public services to citizens (e-Government) has grown to be an integral part of the European reality.[4] A public service is *"any public sector service exposed to a cross-border dimension and supplied by public administrations, either to one another or to businesses and citizens in the Union"*.[5] The EU's e-Government approach is to encourage and expect online public services that are designed to be *"digital by default"*.[6] e-Government is considered to be bringing about advantages in cost savings and the reduction of administrative burdens, and to encourage citizen participation by providing better efficiency and transparency.[7] Thus, the EU has set a handful of goals to encourage the growth of online public services.[8] The backbone

[3] European Commission, *"A Digital Agenda for Europe"* (Communication) COM (2010) 245 final, s 1.

[4] European Commission, *"Towards interoperability for European public services"* (Communication) COM(2010) 744 final, s 1.2.

[5] Directorate-General for Informatics (European Commission), *"New European Interoperabiliity Framework; Promoting seamless services and data flows for European public administrations"* (Publications Office of the European Union 30 November 2017) DOI: 10.2799/78681 7.

[6] European Parliamentary Research Service, *eGovernment: Using technology to improve public services and democratic participation* (PE 565.890, 2015) ⟨http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA(2015)565890_EN.pdf⟩ accessed 25 May 2019 (archived at ⟨https://archive.fo/O4xX3⟩) 4.

[7] ibid 4–6.

[8] *See* the *"Digital by Default"*, the *"Once only principle"*, the *"Inclusiveness and accessibility"*, the *"Openness and transparency"*, the *"Cross-border by default"*, the *"Interoperability by default"* and the *"Trustworthiness and Security"* goals in: European Commission, *"EU eGovernment Action Plan 2016–2020"* (Communication) COM (2016) 179 final, s 2.

of these online public services is the *"European Interoperability Framework"*,[9] with the newest version, called the *"new European Interoperability Framework"*, released in 2017.[10]

The (new) European Interoperability Framework *"is a commonly agreed approach to the delivery of European public services in an interoperable manner."*[11] Interoperability is conceived as the ability of these services to work *"towards mutually beneficial goals, involving the sharing of information and knowledge [...] by means of the exchange of data between their ICT systems."*[12] The European Interoperability Framework *"defines basic interoperability guidelines in the form of common principles, models and recommendations."*[13] The interoperability guidelines, updated in 2017, set out three goals for European public services:

- *improve their national governance of interoperability activities,*
- *use common operational models to develop better digital public services and include the needs of citizens and businesses from other EU Member States,*
- *manage data they own in common semantic and syntactic formats to make it easier to publish it on portals, and to aggregate, share and reuse it.*[14]

At the same time, the EU recognises that advances in e-Government increase the risk to citizen's privacy,[15] and has set up initiatives to increase the trust and take-up of digital services.[16] An essential element of online trust has been deemed the use of electronic identity information.[17] The European Commission has decided to accelerate the use of Electronic Identification (eID) for digital services between Member States in cross-border and cross-sector scenarios,[18] by updating and extending the European Interoperability Framework.[19]

[9] Not to be confused with the *eIDAS Interoperability Framework*, see text of n 64. The new European Interoperability Framework has been updated to conform to eIDAS (see European Commission, *"European Interoperability Framework – Implementation Strategy"* (Communication) COM (2017) 134 final, fn. 14 and related), but its scope is the interoperability of all public administrations in the EU. In the remainder of this thesis, 'Interoperability Framework' will refer to the eIDAS Interoperability Framework.

[10] ibid 3. The 'new European Interoperability Framework' is the third version of the framework, which was first introduced in 2004 (IDABC, *European Interoperability Framework for Pan-European eGovernment Services* (v1.0, 2004) ⟨https://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529⟩ accessed 6 January 2020), subsequently updated in 2010 (European Commission, *"Towards interoperability for European public services"* (Communication) COM(2010) 744 final, Annex 2) and re-confirmed in EU's Digital Single Market Strategy in 2015 (European Commission, *"A Digital Single Market Strategy for Europe"* (Communication) COM (2015) 192 final, s 2.2.3).

[11] Directorate-General for Informatics (European Commission) (n 5) 2.

[12] ibid 2.

[13] ibid 2.

[14] COM (2017) 134 final (n 9) 4.

[15] European Parliamentary Research Service (n 6) 7.

[16] COM (2016) 179 final (n 8) s 2.

[17] European Parliamentary Research Service (n 6) 18.

[18] COM (2016) 179 final (n 8) s 3.1.

[19] COM (2015) 192 final (n 10) s 4.2.

eID,[20] also commonly referred to as 'entity authentication',[21] is *"the process of using claimed or observed attributes of an entity to deduce who the entity is."*[22] An entity is any natural or legal person. An attribute is *"a distinct, measurable, physical or abstract named property belonging to an entity."*[23] In other words, the name, address or date of birth of a natural person are attributes of that person. Electronic identification works by comparing a set of claimed attributes to a set of observed attributes (authentication assertion) through the process of authentication.[24] Because the comparison is performed through electronic representations of attributes (i.e. not by physical examination), a threshold exists after which the electronic representations are considered to be genuine and valid. This threshold is called a *"level of confidence"*.[25] The electronic representation of attributes is stored in a software or hardware token[26] (e.g. a username & password combination; a chip & PIN card). These tokens are referred to as eID tokens or eID means.

eID solutions are not uniform. With standardisation and regulation lagging behind,[27] public services are free to set their own criteria over which eID technology they will deploy. In practice, this has created a diverse landscape, where different solutions exist between national or even between local levels.

In a report commissioned in 2013, the authors noted that

> *[o]ne of the major factors blocking the development of interoperable identity management systems across Europe is the diversity (and, often, incompatibility) of technical and mainly legal approaches to the protection and management*

[20] This thesis will be using the terminology as set up by *eIDAS*, art 3; however, some basic concepts relating to the process of electronic identification (eID) are hereby explained by reference to the Common Terminological Framework set up in Modinis IDM Study Team (ed), *Common Terminological Framework for Interoperable Electronic Identity Management* (techspace rep, 2.01, Europäische Gemeinschaft - eGovernment Unit 2005) ⟨https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf⟩ accessed 17 January 2020 (archived at ⟨https://tinyurl.com/yxyt942w⟩). For consistency, a glossary of terms has been included, with reference to both sources where applicable.

[21] See e.g. Audun Jøsang, *"Assurance Requirements for Mutual User and Service Provider Authentication"* (Joaquin Garcia-Alfaro and others eds, Springer International Publishing 2015); Edgar Whitley and Gus Hosein, *"Global Challenges for Identity Policies"* (plagrave macmillan 2010) DOI: 10.1007/978-0-230-24537-2.

[22] Modinis IDM Study Team (n 20) para 4.18.

[23] ibid para 4.4.

[24] *"Entity authentication is the corroboration of the claimed identity of an entity and a set of its observed attributes."* ibid para 4.5.2.

[25] *"Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence."* ibid para 4.5.

[26] *"A token is any hardware or software that contains credentials related to attributes."* ibid para 4.42.

[27] Approximately 22 standards, often time competing, have been developed so far relating to (aspects of) eID by different bodies. However, most of these attempts are a development of the past decade: Tariq Malik and Anita Mittal, *Technical Standards for Digital Identity Systems for Digital Identity* (World Bank Group's draft for discussion, 2017) ⟨http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf⟩ accessed 5 January 2020 (archived at ⟨https://tinyurl.com/ycegq9tm⟩) 32–37.

> *of electronic identities by EU Member States.*[28]

An attempt to harmonize the eID solutions across the bloc would, therefore, prove impossible. Firstly, because it would imply that Member States with vastly different or incompatible eID schemes would be forced to recall their eID solutions. Secondly, because where eID involves the use of official electronic documents or credentials (e.g. eID national cards) the EU does not have regulatory competence.[29] Instead, the EU pushed for the interoperability of eID across borders through mutual recognition by the Member States of their respective eID schemes.[30] In 2014 the Regulation (EU) No 910/2014 on Electronic Identification And Trust Services (eIDAS)[31] was enacted, and became directly applicable on 1 July 2016.[32]

eIDAS' main objective is to establish the interoperability of eID schemes.[33] eIDAS applies to public-sector services,[34] for example revenue and customs authorities offering an online tax payment service. In contrast, the use of eID in private settings, such as for example the use of eID means for employees to access buildings of private companies,[35] falls outside the scope of eIDAS. eIDAS aspires, however, to create incentives for the voluntary participation of the private sector.[36] The mutual recognition of eID schemes

[28] Martin Becerra Gomes de Andrade and others, *Electronic Identity in Europe: Legal challenges and future perspectives (e-ID 2020)* (EUR 25834, 2013) DOI: 10.2791/78739 16.

[29] *"Identity management as such in relation to official eIDs falls under the subsidiarity of Member States."*: European Commission, *"IMPACT ASSESSMENT: Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market "* (Commission staff working paper) SWD(2012) 135 final, 20. For a discussion on the difficulty to establish legal action in the field of eID, see Norberto Nuno Gomes de Andrade, *"Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID"* (2012) 28(2) Computer Law & Security Review 153 DOI: 10.1016/j.clsr.2012.01.012.

[30] Based on the removal of existing barriers to the functioning of the internal market pursuant of Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ L326/47 (TFEU) art 114: European Commission, *"Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Text with EEA relevance)"* COM (2012) 238 final, 3.

[31] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

[32] With the articles on notification of eID schemes and the Interoperability Framework becoming directly applicable from as early as 17 September 2014 and mandatory recognition starting on 29 September 2018: ibid art 52(2).

[33] ibid rec 12: *"One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services."*

[34] ibid art 6(1).

[35] Such is the case in Belgium, with the eID card 'BelPic': Jan van Arkel, Marc Lange, and Henry Ryan, *Towards an electronic ID for the European Citizen, a strategic vision: CEN/ISSS Workshop eAuthentication* (0.17, 2004) ⟨https://danishbiometrics.files.wordpress.com/2009/08/doc.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/rrykxr8⟩) 33.

[36] eIDAS (n 31) rec 17: *"Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions."* European Commission, *"Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe"* (Communication) COM(2016) 288 final, 11 *"The aim will be to encourage online platforms to recognise other eID means – in particular those notified under the eIDAS Regulation"*.

occurs after a notification process.[37] Although eIDAS often refers to eID schemes as *"national electronic identification schemes"*,[38] eligible for notification are all schemes issued or endorsed by a Member State in order to access at least one public-sector service.[39] In other words, a Member State may notify more than one eID schemes and it may notify schemes of regional rather than national reach.[40] There is no limit on the number of schemes a Member State can notify. eIDAS aims to follow a technology-neutral approach,[41] offering minimum requirements for interoperability instead of rigid technical specifications for the operation of eID.

eIDAS uses a slightly different terminology to the *Common Terminological Framework for Interoperable Electronic Identity Management* that was developed for the Commission back in 2005.[42] Authentication, i.e. the process of comparing the claimed identity to the attributes stored in an eID token, is defined as *"an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed"*.[43] eID is defined as *"the process of using person identification data in electronic form uniquely representing either a natural or legal person,"*[44] in other words eIDAS departs slightly from the eID definition given previously[45] by requesting the 'unique' representation of a person.[46] The attributes representing a person are called *"person identification data"*.[47] The attributes are held in *"electronic identification means"*,[48] i.e. eID means (or eID tokens). An eID means can be, for example, a physical ID card with an electronic chip. The chip holds an electronic representation of the person identification data written on the ID card (such is the case in Germany). Or, taking the example of the UK, an eID means can be software-based only: a set of person identification data stored on a server and accessed through a username/password combination. Four actors are involved in an eID process:

(a) a citizen of Member State A using their eID means to authenticate to a service;

[37] eIDAS (n 31) art 9.

[38] See e.g. ibid art 12(1).

[39] ibid arts 7(a) and 7(b).

[40] For example, the 'Digital Identity Scotland' being developed (https://blogs.gov.scot/digital/2019/01/21/online-identity-assurance-introducing-digital-identity-scotland/) for access to Scottish public services would fulfil the eligibility criterion of ibid art 7(b) even though it is separate from the UK's national eID scheme 'Gov.UK Verify'.

[41] ibid rec 4.

[42] See text nn 20 to 26.

[43] eIDAS (n 31) art 3(5).

[44] ibid art 3(1).

[45] See n 22.

[46] See n 145.

[47] *"a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established"*.eIDAS (n 31) art 3(3).

[48] *"a material and/or immaterial unit containing person identification data and which is used for authentication for an online service"* ibid art 3(2).

(b) the citizen's eID scheme,[49] that has issued the eID means and is being used to perform the authentication;

(c) the eIDAS Interoperability Framework that translates the data from the eID scheme of Member State A to the eID scheme of Member State B; and

(d) a *"relying party"* in Member State B,[50] which is the public sector body[51] that offers the service to the citizen of Member State A (i.e. a Service Provider).

An overarching requirement is that all processing undertaken by eID schemes under eIDAS shall conform to the Data Protection Directive[52] (Dir 95/46/EC).[53] However, EU's framework of personal data protection has since been updated by the General Data Protection Regulation (GDPR).[54] Dir 95/46/EC has been repealed from 25 May 2018[55] and all references to Dir 95/46/EC shall now be interpreted as references to the GDPR pursuant to GDPR Article 94(2).[56] The GDPR has updated and strengthened the protection of personal data in the EU, introducing several novel requirements.[57]

1.1 The Motivation behind this Research

Data protection is paramount for the success of eID within the EU.[58] In fact, eIDAS recognises the importance of data protection by explicitly mentioning the applicable data protection legislation on two different occasions: A general requirement for all personal data processing to be performed in compliance with data protection legislation,[59] and, a

[49] *"a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons"* eIDAS (n 31) art 3(4).

[50] *"a natural or legal person that relies upon an electronic identification"* ibid art 3(6).

[51] *"a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services"* ibid art 3(7).

[52] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31.

[53] eIDAS (n 31) art 5(1).

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[55] ibid art 94(1).

[56] With a two-year window for data controllers and data processors to adjust any processing already underway to conform to the GDPR: ibid rec 171.

[57] As de Hert and Papakonstantinou note *"incorporating the lessons learned over more than fifteen years of rigorous implementation, and updating the assumptions in contemporary processing circumstances. Among its novelties are the introduction of a 'right to be forgotten' and a 'right to data portability,' the application of Privacy By Design system architecture, the introduction of a 'principle of accountability' intended to levy the bureaucratic burden off data controllers, and the introduction of 'data protection impact assessments.'"* Paul de Hert and Vagelis Papakonstantinou, *"Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?"* (2013) 9(2) A Journal of Law and Policy for the Information Society 271 , 312.

[58] COM (2016) 179 final (n 8) s 2.

[59] eIDAS (n 31) art 5(1).

specific obligation for compliance of any personal data processing performed within the eIDAS Interoperability Framework.[60] The updated regime under the GDPR reinforces the data protection rights of individuals and makes explicit the risk-based approach to the protection of personal data,[61] as evidenced by the introduction of a balancing test in Article 25.[62]

A starting point for this thesis was, therefore, to study the interplay between the GDPR and eIDAS through a preliminary research question:

What is the impact of the GDPR on eIDAS and is eID under eIDAS consistent with the GDPR?

eIDAS defines a minimum common denominator that all eID schemes should conform to in order to interoperate, by imposing minimum requirements for compliance. The requirements are presented as a set of high-level principles and objectives which, in principle, should not restrict the way they are accomplished.[63] Under Article 12, an EU-wide eIDAS 'Interoperability Framework' is established.[64] The Interoperability Framework is a set of technical requirements,[65] required attributes representing a natural or legal person,[66] procedural rules,[67] dispute resolution arrangements,[68] and common security standards.[69] This set of requirements is considered necessary for successful communication between the eID schemes. In other words, the Interoperability Framework can be considered as a layer that will perform a translation between the diverse eID schemes. The translation will transform the attributes (the eID means) used by an eID scheme to a common data format so that it is comprehensible by other eID schemes.

[60] ibid art 12(3)(d).

[61] Dir 95/46/EC did not contain explicit mentions to a risk-based approach. However, The Court Of Justice Of The European Union (CJEU) has confirmed the existence of a balancing test on a number of cases. See, e.g. Judgement of 19 October 2014, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, EU:C:2016:779, para 62; Judgement of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16, EU:C:2017:336 and especially Opinion of 26 January 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16, EU:C:2017:43, paras 60-68.

[62] See text of n 83. For an interesting discussion on the existence of the balancing test *cf.* Raphaël Gellert, *"We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection"* (2016) 2(4) European Data Protection Law Review 481 Bart van der Sloot, *"Editorial"* (2017) 3(1) European Data Protection Law Review 1 DOI: 10.21552/edpl/2017/1/3 and Raphaël Gellert, *"On Risk, Balancing, and Data Protection: A Response to van der Sloot"* (2017) 3(2) European Data Protection Law Review 180 DOI: 10.21552/edpl/2017/2/7.

[63] eIDAS (n 31) art 12(3)(a): *"it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;"*.

[64] ibid art 12(2). This is distinct from the *"new Interoperability Framework"* of n 10 that concerns all aspects of interoperability for public administrations in the EU. The eIDAS Interoperability Framework (hereinafter 'Interoperability Framework') targets only the interoperability between eID and trust services.

[65] ibid arts 12(4)(a–c).

[66] *"person identification data"* ibid art 12(4)(d).

[67] ibid art 12(4)(e).

[68] ibid art 12(4)(f).

[69] ibid art 12(4)(g).

Participation of eID schemes follows a notification procedure,[70] where the notifying Member State informs the EU Commission of its intention to allow its eID means to be used for authentication in other Member States. A successful notification presupposes a demonstration of how the eID scheme in question satisfies the Interoperability Framework's requirements,[71] and a classification of the eID scheme against one of the three *"assurance levels".*[72] The assurance levels describe different degrees of confidence in the accuracy of the claimed identity, divided into *"low"*, *"substantial"* and *"high".*[73] EU Member States are required to automatically recognise successfully notified eID schemes of levels *"substantial"* and *"high".* Recognition of notified schemes of level *"low"* is voluntary.[74] Recognition is irrespective of whether the recognising Member State has notified their own eID scheme. Member States have otherwise freedom in the architectural design of the schemes,[75] provided that the design does not contradict the specifications set forth by eIDAS[76] and does not impose disproportionate technical obligations to foreign Member States.[77]

The freedom of design, compounded with additional implementation requirements added by eIDAS' subsequent Implementing Regulations[78] create a complex landscape. The complexity makes it difficult to identify the areas where eIDAS' requirements would have to be expanded by obligations and rights set forth by the GDPR and to assess whether the additional requirements of the implementation acts are consistent with the GDPR. In answer to these considerations, chapter 3 performs a classification of applicable requirements from eIDAS and the GDPR in the field of eID. Extracted requirements are grouped into categories according to their *ratio legis*, i.e. the purpose they aim to serve. The eIDAS categories are then compared to the GDPR categories. It is discovered that in most cases, eIDAS and the GDPR requirements complement each other. There is,

[70] eIDAS (n 31) art 9(1).

[71] nn 65 to 69.

[72] eIDAS (n 31) art 8.

[73] The equivalent of the *"levels of confidence"* described in n 25.

[74] eIDAS (n 31) art 6(2).

[75] ibid rec 12: *"This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States."*

[76] ibid art 7.

[77] ibid art 7(f).

[78] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1; Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/7; Commission Implementing Regulation (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2015] OJ L289/18; Commission Implementing Regulation (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2015] OJ L53/14.

however, an overlap between two categories: (a) requirements in regard to liability, and, (b) requirements in regard to data protection by design.

In the areas of overlap the two legal instruments are seemingly competing, with the GDPR containing stricter requirements. The question becomes, therefore, whether eIDAS can satisfy the stricter requirements of the GDPR. Notably, this is not a question about which of the two legal instruments should apply: As explained further in chapter 3 section 3.5, where eID schemes within the Interoperability Framework process personal data, they will have to meet the obligations set forth by the GDPR. This conclusion is not only supported by the explicit admission of Articles 5(2) and 12(3)(d) that eIDAS should not derogate from data protection obligations.[79] The GDPR targets a narrower subject matter (personal data) and was adopted after eIDAS. Further, eIDAS cannot be considered as a 'self-contained regime' that would be seen as *lex specialis* over the GDPR.[80] Accordingly, in the areas of liability and data protection by design eIDAS' requirements shall accommodate the obligations of the GDPR – where personal data are involved.

Regarding liability, eIDAS' liability regime for eID intends only to identify the responsible party in complex scenarios of multi-party eID provision (i.e. where the party issuing the eID means is different to the party performing the authentication) and does not prescribe rules of burden of proof or redress. As such, the liability regimes from eIDAS and the GDPR can work in parallel.[81]

However, accommodation of data protection by design requirements is harder. Under GDPR Article 25, data controllers are required to take appropriate technical and organisational measures to ensure that data protection principles are implemented from the determination of the means and throughout the data processing. Although undoubtedly this includes the principles of Article 5, on closer inspection Article 25 brings in other GDPR obligations as well.[82] The prescription of data protection by design by the GDPR is contextual: the measures shall be proportionate to *"the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing".*[83] Article 25 offers data minimisation as an example of the pursued goals and pseudonymisation as an example of appropriate measures.

On the other hand, eIDAS (and its implementing acts) establishes similar but different concepts: the 'facilitation' of privacy by design[84] and the non-prohibition of the use of pseudonyms.[85] Data minimisation is effected under eIDAS through the definition of

[79] n 177.
[80] n 180.
[81] Text of n 331 and related discussion.
[82] Text of n 358.
[83] GDPR (n 54) art 25(1).
[84] eIDAS (n 31) art 12(3)(c).
[85] ibid art 5(2).

"a minimum set of person identification data uniquely representing a natural or legal person".[86] This 'minimum dataset' was considered as the minimum necessary in order for successful eID operation.[87] Most importantly, the architecture of the Interoperability Framework, the format of the person identification data and the security safeguards in place are determined by subsequent implementing acts, which create *de facto* architectural limitations. And the Interoperability Framework will interact with eID schemes of varying architectures (i.e. of varying levels of data protection by design).

As a result, contextualising data protection by design within the Interoperability Framework is not a straightforward exercise. eIDAS defines an explicit set of personal data to be collected (the Minimum Dataset) and the safeguards for its protection through the establishment of the Interoperability Framework. Determining an explicit set to be processed in all cases should be assessed against the requirements of data protection by design under the GDPR. In order to successfully understand whether the operation of the Interoperability Framework supports an adequate level of data protection by design, there is a need to first unpack GDPR Article 25's requirements and then assess them against the Interoperability Framework. Chapter 4 to chapter 9 examine the scope of GDPR Article 25, the minimum approach applied by eIDAS in its cooperation with the participating eID schemes and whether the level of data protection by design that can be achieved under eIDAS is satisfactory to the GDPR. The research question, thus, in light of chapter 3, now becomes:

Is the level of data protection by design that can be achieved by eIDAS' Interoperability Framework enough to satisfy the requirements of GDPR Article 25?

1.2 Scope and Limitations of this Thesis

In light of the above, this thesis examines what data protection by design entails in the context of interoperable EU eID. The purpose is to assess the current level of data protection by design afforded by the eIDAS Interoperability Framework and determine its conformity to the legal requirements of GDPR Article 25. The objectives, therefore, are:

a to clarify the substance of data protection by design under GDPR Article 25;

[86] eIDAS (n 31) art 12(4)(d).

[87] See SWD(2012) 135 final (n 29) 33 *"...limited to the unambiguous link between the identification data attributed to a person via the eID (e.g. person data such as name, date of birth and person identifier such as tax number in Italy, or the residence register in Austria). This ensures that each individual can be uniquely identified, even if some attributes are shared (e.g. multiple John Smiths, who may even share the same date of birth or city of residence)."*

b to derive data protection requirements as a pre-condition for data protection by design compliance;

c to assess the current specifications of eIDAS against the data protection by design requirements;

d to determine the conformity of the Interoperability Framework to GDPR Article 25 and analyse the implications.

Notably, this thesis only examines eID schemes that fall within the scope of eIDAS, i.e. schemes that are used in a Member State in order to access public-sector services and are, or will be, notified under the notification procedure of eIDAS Article 9. Further, it only examines data processing that falls within the scope of the GDPR. Risk for the purposes of this thesis should be understood as data protection risk, i.e. risks to the rights and freedoms of individuals,[88] which is different than security risk and cybersecurity. The thesis examines data protection by design, namely the measures and safeguards that are to be engineered into the processing.

A distinction should be noted here between data protection by design and data protection by default.[89] Data protection by design is specified in GDPR Article 25(1) and expresses the obligation of the data controller to *"put in place appropriate technical and organisational measures designed to implement the data protection principles; and integrate safeguards into your processing so that you meet the GDPR's requirements and protect the individual rights."*[90] Data protection by default in GDPR Article 25(2), on the other hand expresses the obligation of the data controller to *"specify this data before the processing starts, appropriately inform individuals and only process the data [needed] for [the] purpose".*[91] In other words, the two operate in parallel: the second principle ensures the capabilities developed as a result of the first principle are the default setting and any changes occur after agreement by the data subject. Hence, both shall be seen in unity and will require the engineering of the data protection principles. However, this thesis only examines data protection by design. It is assumed that the *"by design"* measures and safeguards examined will be set to on *"by default".*

The objectives a–d are examined in chapters 4 to 9. Firstly, the exact prescription of GDPR Article 25 is analysed. The analysis starts from the origins and evolution of the concept of data protection by design. Aspects of the concept emerged in the early '70s, and have been refined and reformed as an (informal) data protection principle until

[88] *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage"*: GDPR (n 54) rec 75.

[89] ibid art 25(2).

[90] ICO, *Guide to the General Data Protection Regulation* (1,0,154, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf⟩ accessed 24 May 2018 (archived at ⟨https://tinyurl.com/y9pr9o2x⟩) 173.

[91] ibid 173.

their formal introduction in the GDPR. It is explained, however, that data protection by design under the GDPR is not straightforward because the obligations it introduces need qualification. A look at the domain and effects of Article 25 reveals that for a correct prescription a double balancing exercise needs to be performed: The benefits of a specific data processing against the risks to the rights and freedoms of the individuals, and tested again against the state of the art and the cost of implementation. Hence, Article 25 shall be read in light of Article 35 on Data Protection Impact Assessments (DPIAs). After taking into account all qualifying factors, it becomes apparent that the goal is not to achieve data protection by design, but rather to achieve *an adequate level* of data protection by design for a specific data processing.

Therefore, the next step is to look to Impact Assessment frameworks and determine how they can be used to assess data protection by design levels. The thesis examines three DPIA methodologies as they have been designed by the Data Protection Authorities (DPAs) of France, Germany and the UK. It was important for any selected methodologies to be from an authoritative source,[92] contain in-depth guidance and templates,[93] and to be able to be applied to eID (i.e. not sector specific).[94] The three methodologies were the only available in the English language at the time of writing.[95] The examination of the three methodologies revealed that the evaluation of the risks needs to go beyond the data protection principles of GDPR Article 5 into various obligations that can be grouped together into 7 categories: data minimisation; data availability; data integrity; data confidentiality; linkages between datasets (unlinkability); transparency of processing; data subject rights (intervenability). Further, even though DPIAs are triggered only when high risks are present, a preliminary test (a threshold analysis) will most likely be required to determine whether a specific processing presents high risks. However, as regards data protection by design, it is doubtful whether existing DPIA frameworks are suitable. DPIA methodologies are useful but rely on the presumption that all the particulars of the processing in question are known. This is not always the case at the starting stages of a processing, when data protection by design measures are meant to

[92] Cf. privately developed models e.g. Kim Wuyts and Wouter Joosen, *LINDDUN privacy threat modeling: a tutorial* (CW reports, CW685, Department of Computer Science, KU Leuven 2015) ⟨https://7e71aeba-b883-4889-aee9-a3064f8be401.filesusr.com/ugd/cc602e_f98d9a92e4804e6a9631104c02261e1f.pdf⟩ accessed 7 January 2020.

[93] Cf. e.g. Gibraltar Regulatory Authority, *(4) Data Protection Impact Assessments* (Guidance note, IR04/17 (v2), 2019) ⟨https://www.gra.gi/download/1020/GDPR4.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ydaukuqv⟩).

[94] Cf. sector specific frameworks e.g. for RFID applications Article 29 Data Protection Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (WP 180, 2011); for smart metering systems European Commission, *"On the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems"* (Commission Recommendation) 2014/724/EU; Smart Grid Task Force, *Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment* (v. 2, 2018) ⟨https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ycj5l9vv⟩).

[95] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev 01, 2017) 20.

be decided and implemented. Unknown variables would preclude being able to follow a DPIA framework in full. It is proposed instead that for the purposes of data protection by design, a threshold analysis similar to the one required to determine the presence of high risks should be applied.

Based on the 7 categories of obligations, a threshold analysis applicable in the field of eID is constructed. The analysis is then applied to the Interoperability Framework. The analysis reveals that eIDAS and its implementing acts might impede three areas: transparency obligations, intervenability obligations and unlinkability obligations. The risks to transparency and intervenability are somewhat mitigated by the discretion allowed to the participating eID schemes to apply the required controls themselves. However, it is shown that linkability risks are not as easy to mitigate. Unlinkability refers to a set of controls (safeguards) that prevent or hamper the aggregations of data sets. The main unlinkability controls are the substitution of attributes by random values (pseudonymisation) and the minimisation of transmitted attributes on a case by case basis (selective disclosure).[96] It is shown that, consistent with the approach in the GDPR,[97] pseudonymisation cannot effect unlinkability without selective disclosure. Even though in principle eIDAS permits pseudonyms, it is demonstrated that pseudonymisation and selective disclosure within the Interoperability Framework are impossible because of a narrow conception of data minimisation. As a result unlinkability is seriously restricted by eIDAS.

In order to understand the effects of the unlinkability limitation on the level of data protection by design, the thesis then examines current implementations of eID. Three national implementations of eID were selected. The three eID schemes are all promoted as privacy-enhancing eID management systems. However, they are each designed according to different architectural models and utilise different methods to tackle unlinkability. It is discovered that all examined eID schemes implement some form of pseudonymisation and data minimisation. Pseudonymisation coupled with full selective disclosure, as achieved by one of them, should be considered the state of the art.

To critically evaluate the analysis, a round of interviews with experts in the field of eID was conducted. The qualitative data supported the assertion that pseudonymisation requires selective disclosure to successfully address linkability risks and that modern eID schemes are working towards this goal. It also endorsed the conclusion that there is currently a threshold of unlinkability within the Interoperability Framework. As a direct consequence, eID schemes that participate in eIDAS are not permitted to surpass this threshold, resulting in a lower level of unlinkability – and hence a lower level of data protection by design – than what certain national eID schemes are able to achieve.

[96] For example, in a scenario where a service can only be provided to adults in the UK, a service would strictly require to know the location and age of the user. The two attributes can subsequently be masked to reveal e.g. municipality instead of address and decade instead of date of birth.

[97] GDPR (n 54) art 4(5).

1.3 The Original Contribution of this Thesis

This thesis began on the premise that, with the advent of the GDPR, the references in eIDAS to Dir 95/46/EC and the requirements to conform to data protection obligations need to be revisited. It showed that the two legal instruments should be read side by side, but the areas of liability and data protection by design require clarification. And though a reconciliation of the liability provisions from both instruments is possible, deciding if eIDAS satisfies the principle of data protection by design is not straightforward. Although data protection by design is not a novel concept in the field, this thesis demonstrated that its particular formulation pursuant to Article 25 makes compliance conditional on the satisfaction of a double balancing exercise. Consequently, an attempt to assess eIDAS' compliance with data protection by design must necessarily assess the benefits and risks of processing against the cost of implementation and the state of the art. Therefore, this thesis posits that data protection by design compliance is a continuum whereby eIDAS needs to achieve a level adequate for the protection of the personal data at stake. The thesis addresses the present absence of methodologies to assess data protection by design by tailoring a threshold analysis specifically for data protection by design, and subsequently tests its application in the assessment of eIDAS' Interoperability Framework.

It determines that, although eIDAS attempts to strike a balance between data protection by design and the requirements for successful cross-border eID, the current level of data protection by design achieved within the Interoperability Framework falls short, especially with respect to unlinkability safeguards. It argues that the level of unlinkability that can currently be achieved is not enough to satisfy compliance with GDPR Article 25. This is especially true in two situations: Firstly, in comparison to the state of the art, as can be achieved by national eID implementations. In the cases where national eID schemes have implemented unlinkability safeguards, their participation in the Interoperability Framework will have the effect of immediately lowering the level of data protection by design they provide. Secondly, because of the Commission's ambition for eIDAS to serve as the basis for the (voluntary) participation of private-sector services. It will be hard to argue that private-sector services require all the attributes present in the Minimum Dataset in order to function successfully. There is a host of private online services, for example online platforms, where the transmission of the Minimum Dataset as defined in eIDAS will be overkill to achieve their purpose. In both cases, lowering the level of data protection by design that can be achieved by the participating eID schemes should not only be seen as violating GDPR Article 25, but also as going directly against the instruction that the Interoperability Framework shall *"facilitat[e] the implementation"*[98] of data protection by design.

[98] eIDAS (n 31) art 12(3)(c).

Consequently, this thesis proposes a practical solution to alleviate incompatibilities with GDPR Article 25. The design of the Interoperability Framework should be amended to enhance the level of data protection by design currently supported. This can be implemented at the 'eIDAS nodes', the hardware and software components of the Interoperability Framework that provide the translation layers to the eID schemes. The eIDAS nodes can be extended to permit full selective disclosure and pseudonymisation, allowing therefore the eID schemes that implement them to be able to maintain a high level of data protection by design across borders. This extension can be effected by a Regulatory Technical Standard (RTS).[99]

1.4 Outline of this Thesis

The rest of the thesis is structured as follows:

Chapter 2 describes the overall methodology followed in this research, explaining how a triangulation of methods (desk research – use cases – qualitative data analysis) was necessary to answer the research question;

Chapter 3 presents the systematic interpretation of how eIDAS and the GDPR should be combined. The analysis revealed that the parallel application of the two creates a tension for data protection by design. This outcome refined the research question and provided the focus for the rest of the research;

Chapter 4 investigates the substance of data protection by design and explains why the formulation of Article 25 requires a parallel reading of GDPR Article 35 *(obj.* a*)*;

Chapter 5 compares the methodologies to perform the assessment of GDPR Article 35 *(obj.* b*)*;

Chapter 6 composes a threshold analysis framework based on the results of the previous chapter and applies it to the eIDAS Interoperability Framework. The assessment reveals that the area of unlinkability is problematic in the current specification of the Interoperability Framework *(obj.* c*)*;

Chapter 7 explains the goal of unlinkability and its necessary components and analyses the limitations of the Interoperability Framework *(obj.* d*)*;

[99] RTSs are delegated acts pursuant to Art 290 TFEU in areas where unduly complicated regulation and enforcement is unnecessary. They *"further develop, specify and determine the conditions for consistent harmonisation of the rules included in the legislative acts adopted by the European Parliament and the Council, supplementing or amending certain non-essential elements thereof."* Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014 Amending Directives 2003/71/ec and 2009/138/ec and Regulations (EC) No 1060/2009, (EU) No 1094/2010 and (EU) No 1095/2010 in Respect of the Powers of the European Supervisory Authority (European Insurance and Occupational Pensions Authority) and the European Supervisory Authority (European Securities and Markets Authority) [2014] OJ L153/1, rec 11.

Chapter 8 examines three national eID implementations to determine the state of the art in the field of eID in particular in relation to unlinkability *(obj.* d *)*;

Chapter 9 evaluates the findings of chapters 6 to 8 through a series of expert interviews *(obj.* d *)*;

Chapter 10 discusses the upshot of the analysis, explains the implications of the limitations of the Interoperability Framework and proposes a practical solution to increase the level of data protection by design;

Finally, chapter 11 summarises the concluding remarks.

Chapter 2

Methodology

2.1 Introduction

Traditional legal research is based on the doctrinal method, which uses legal reasoning techniques for a systematic interpretation of legal rules. Although the doctrinal method has been extensively used in parts of this thesis, in order to reach the research objectives it was complemented by empirical research methods. This decision was based on the substantive analysis of the overlap between eIDAS and the GDPR.

Having determined through doctrinal research that the two regulations will apply in parallel, as shown in the next chapter, the question that arose concerned the effects of data protection by design on eIDAS' Interoperability Framework. Data protection by design is by definition a mixture of policy and technological measures. Further, its prescription under the GDPR is directly dependant on contextual factors. It was decided, therefore, that an interdisciplinary assessment of data protection by design was required: legal research methods in order to examine the interplay between the rules of eIDAS and data protection by design, and empirical research methods with a focus on privacy enhancing technologies in order to contextualise data protection by design for eID.

Hence, in addition to the legal reasoning methods, case studies on national eID schemes were conducted. The selected case studies revealed the state of the art in relation to the field of eID and assisted in extrapolating the implications of participation within eIDAS' Interoperability Framework for national eID schemes.

To mitigate limitations of internal and external validity of the study, the methods above were triangulated with qualitative data from in-depth expert interviews. The interviews were used to evaluate the analyses and the findings produced at the doctrinal and case study phases.

The overall study design took into account the inherent limitations of each method. Mitigating safeguards have been implemented through the design of the methods and their triangulation. The combination of the findings from the three methods was used in the final discussion of the analysis and permitted the development of a practical solution to extend support for data protection by design.

Below, section 2.2 explains the reasons why this study follows an interdisciplinary mixed methods approach. Section 2.3 describes each of the methods selected for this mixed methods approach.

2.2 The Rationale behind the Chosen Method

This thesis started with the goal to explore the effects of the GDPR on eIDAS. The study had as a starting point, therefore, the intersection between eIDAS and the GDPR, i.e. the intersection between two legal instruments of EU law. Traditional black letter legal research is based on the doctrinal method. Doctrinal research uses legal reasoning to form legal arguments that, when applied, allow the researcher to develop a deep understanding of an authoritative text.[100] Hence, the doctrinal method was selected in order to examine the scope and substance of the GDPR and eIDAS and identify their standing in the EU legal order.

Having determined that both instruments are of equal legal standing (i.e. no instrument has priority over the other and they both shall apply in parallel), a classification based on legal reasoning was devised to identify the areas where the two instruments overlap. Accordingly, this interpretative framework narrowed down the scope of the research to one potentially problematic area: the effects of data protection by design on the Interoperability Framework set up by eIDAS.

Data protection by design under Article 25 of the GDPR assumes an approach that relies on the qualification of several contextual factors. These factors can in general be divided into two main categories: (a) factors relating to the legal protection of personal data, and, (b) factors relating to the technical protection of personal data. For example, under (a) fall the nature, scope, context and purposes of processing and the risks to the rights and freedoms of the data subjects. Whereas the state of the art and the cost of implementation fall under (b). Hence, two wide groups need to be considered for adequate understanding of the effects of Article 25 on eIDAS. The exclusive use of the doctrinal legal method would not have been suitable to examine the technical protection.

In areas of underlying complexity, such as this, complimenting legal research methods with empirical methods can offer an external perspective,[101] informing how the law is

[100] Sanne Taekema, *"Relative Autonomy, A Characterisation of the Discipline of Law"* in BMJ van Klink (ed), *Law and Method. Interdisciplinary Research into Law* (Politika 4, Mohr Siebeck 2011) 47.

[101] In contrast to the doctrinal method that studies the 'internal aspect', i.e. *"the internal point of view refers to a specific kind of normative attitude held by certain insiders, namely, those who accept the legitimacy of the rules."*Scott J Shapiro, *"What Is the Internal Point of View?"* (2006) 75(3) Fordham Law Review 1157 , 1159.

applied in practice.[102] Techno-legal aspects such as data protection by design should be approached through interdisciplinary research, which can cross the boundaries of legal research and create new integrated knowledge.[103] For subjects with a variety of perspectives and data a more pragmatic mixed methods strategy is better,[104] allowing the flexibility to select the methods necessary for the objectives of the research.[105]

In the mixed methods approach selected for this thesis, doctrinal research has been used for the substantive analysis of the law. This task depends on doctrinal research because it requires the legal *"interpretation and application of the existing body of knowledge of law and of legal practice".*[106] However, in order to adequately study the other aspects of data protection by design, law, which is a normative discipline, is not enough. As van Klink and Taekema note,[107] inspiration should be drawn by empirical disciplines of organisational studies and sociology. Empirical tools and methods can be used to obtain factual data which, when used in legal studies, can *"reveal, 'the limits of institutional action', 'practical insider attitudes' and 'conceptions and experiences of law and legal institutions'."*[108] In addition, Argyrou notes that when legal scholars want to address the impact of the current law on certain social constructs in practice, *"in epistemological terms, a space is created for the use of empirical legal research."*[109] Hence, empirical research used in a legal context is able to indicate flaws in the effectiveness and implementation of the legislation and suggest necessary changes.

In this thesis, a mixed-methods approach was adopted in line with the objectives of the research.[110] Empirical research was used to show the effectiveness of the law as a tool to achieve a set of policy goals[111] (in this case data protection by design, examined through a threshold analysis). Further, when gaps between the aim and the effectiveness of the legal rule were identified, empirical qualitative research assisted in formulating normative

[102] Aikaterini Argyrou, *"Making the Case for Case Studies in Empirical Legal Research"* (2017) 13(3) Utrecht Law Review 95 DOI: 10.18352/ulr.409, 97.

[103] BMJ van Klink and HS Taekema, *"On the Border. Limits and Possibilities of Interdisciplinary Research"* (BMJ van Klink and HS Taekema eds, Mohr Siebeck 2011) 7.

[104] Joanna EM Sale, Lynne H Lohfeld, and Kevin Brazil, *"Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research"* (2002) 36(1) Quality and Quantity 43 DOI: 10.1023/A:1014301607592, 50.

[105] John W Creswell and Vicki L Plano Clark, *"Designing and Conducting Mixed Methods Research"* (3rd edition, SAGE 2017) 26–27.

[106] Reza Banakar, *"On the Paradox of Contextualisation"* in *Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity* (Springer International Publishing 2015) DOI: 10.1007/978-3-319-09650-6_5 91.

[107] van Klink and Taekema (n 103) 8–9.

[108] Argyrou (n 102) 96 citing Banakar (n 106) 91.

[109] Argyrou (n 102) 97.

[110] Following the tenet of legal realism that *"research methods should be chosen to match the kinds of questions being asked"*: Mark C Suchman and Elizabeth Mertz, *"Toward a New Legal Empiricism: Empirical Legal Studies and New Legal Realism"* (2010) 6 Annual Review of Law and Social Science 555 DOI: 10.1146/annurev.lawsocsci.093008.131617, 562.

[111] Frans L Leeuw, *"Empirical Legal Research: The Gap between Facts and Values and Legal Academic Training"* (2015) 11(2) Utrecht Law Review 19 DOI: 10.18352/ulr.315, 29.

statements out of the empirical findings[112] (in this case how the state of the art achieved the sub-goal of unlinkability for data protection by design, examined through a set of case studies).

Consequently, this research used the doctrinal method for data retrieved from relevant documents and their interpretation; it further used direct observations in case studies and in-depth interviews with experts for qualitative research. In part, the use of case studies was selected because of the requirement to discover the state-of-the-art. As a result, a 'naturalistic' research method, that allowed the examination of social phenomena in their natural setting, was necessary.[113] Case study research can be used to provide explanations and descriptions of the applications of a phenomenon[114] (in this case of data protection by design). Multiple case studies were conducted together for illustrative reasons: the parallel examination allows the comparison of practices and the explanation of differences.[115] Along the same vein, in-depth interviews were selected for their 'participatory' nature,[116] because interviews allow the research subjects to play a crucial role in the confirmation of the analysis.

However, the selection of multiple qualitative methods to complement the doctrinal research was decided also in order to safeguard against the limitations and biases that a single method can introduce. The limitations of case study research in terms of replication and generalisation difficulties were compensated by the performance of multiple case-studies which were then compared and contrasted. The risk of researcher bias when interpreting the findings was mitigated through the external confirmation of the findings during the expert interviews. Interviews also inherently carry risk: there is a chance of unconscious bias towards preconceived notions with the researcher attempting to stir the interviewee towards the preconception. Against this risk, this study selected a semi-structured format for the interviews so that participants were able to express and elaborate on subjects as they saw fit. In order to mitigate any selection bias, the participation threshold was purposefully kept low, with only criterion being their work experience in the field of (national) eID. Finally, the methods and their findings were triangulated to mitigate any risks of the doctrinal research remaining too 'high-level', and hence difficult to produce any tangible results. Triangulation, as defined by Webley, is the process of considering *"as many different standpoints as possible, using as many different data types as possible to permit a holistic examination of the question to see which explanations, if any, remain consistent across all data sources"*.[117] Triangulation not only allowed to identify the most consistent structures and explanations, but also to reinforce

[112] P Chynoweth, *"Legal research"* in A Knight and L Ruddock (eds), *Advanced research methods in the built environment* (Wiley-Blackwell 2008) 30.

[113] Lisa Webley, *"Qualitative Approaches to Empirical Legal Research"* in Peter Cane and Herbert M Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2012) 929.

[114] Robert K Yin, *"Case Study Research: Design and Methods"* (5th, SAGE Publications 2014) 4.

[115] Terry C Hutchinson, *"Researching and writing in law (3rd ed.)"* (Lawbook Co/Thomson Reuters 2010) 104.

[116] Webley (n 113) 928.

[117] ibid 929.

both the internal and the external validity of this study and of its methods.[118] Table 2.1 summarises the various limitations of each method and the mitigating safeguards chosen in this study.

Methodological step	**Limitation**	**Safeguard**
All	Construct, internal, external validity	Triangulation of methods; triangulation of findings
Doctrinal research	Arguments and findings too 'high level'	Triangulation of findings
Case study	Lacks objectivity of quantitative proof	Used as part of a mixed setting
Case study	Researcher bias in interpreting findings	Validation of findings by external researchers
Case study	Difficult to replicate	Combination of multiple case studies
Case study	Difficult to generalise	Multiple case studies and external validation of findings
Interviews	Bias towards verification of preconceived notions	Semi-structured format
Interviews	Lack of representativeness	Selection of experts from different EU states with all types of eID architectures represented
Interviews	'Unreadable' extensive data; bias in interpretation	Transcripts codified by pre-selected scheme; both over- and under-represented schemes discussed in findings
Case study/Interviews	Danger of non-applicability of propositions due to lack of general application	Carefully scoped domain of application (EU cross-border eID)
Case study/Interviews	Selection bias	Selection of case studies of different architecture; selection of experts based only on working experience in the field

Table 2.1: Limitations of the study and methodological safeguards

2.3 The Methodology to Assess the Implications of the GDPR on the Interoperability Framework

This section provides an overview of the methods selected for this research. Further details on specifics are also given in the corresponding chapters as needed.

Doctrinal research has been used in two occasions in this research: First, to clarify the scope of this research and identify the areas of overlap between the GDPR and

[118] Argyrou (n 102) 98.

eIDAS. Second, having determined that the area of focus should be the data protection by design, to investigate the substance of data protection by design and compose the threshold analysis framework used for the assessment of data protection by design in the Interoperability Framework.

In order to clarify the scope, doctrinal research was used to systematically interpret the GDPR and eIDAS. After an analysis using traditional norm-conflict methods, the concept of '*ratio legis*', i.e. the rationale behind a particular legal rule, was used to construct a classification framework. The classification framework comprised seven thematic categories, or goals, that a legal rule contained within the GDPR or eIDAS may pursue. The obligations set forth by the GDPR and eIDAS were classified against this framework. The comparison of the categories revealed that the obligations of data protection by design between eIDAS and the GDPR did not completely align and further examination was needed.

To conduct the examination, this research combined doctrinal research with two additional methods for the analysis, synthesis and evaluation of data protection by design in the Interoperability Framework. Triangulation of measures is particularly useful in case study research,[119] as it can offset potential flaws by corroborating strategies and methods against each other.[120] The overall design plan comprised three parts: Doctrinal research to clarify the substance of data protection by design and derive data protection requirements; case study research of three national eID schemes to assess the state of the art in data protection by design and analyse the impact of the Interoperability Framework on national schemes; in-depth expert interviews to evaluate the analysis. The three methods are depicted in figure 2.1.

The doctrinal research was used to examine the prescription of data protection by design under the GDPR, discover its implications for eID schemes and analyse its current implementation under the Interoperability Framework. For that purpose three categories of sources were examined: eID legislation and policies, including eIDAS and its implementing acts, as well as policy documents from the eIDAS Task Force; EU data protection legislation and guidance, including the GDPR and the guidance issued by the Article 29 Data Protection Working Party (WP29), the European Data Protection Board (EDPB) and national DPAs; and, eID technical specifications, including eID design and architecture, security and privacy literature. The three categories allowed the identification of (a) the legal requirements mandated by eIDAS; (b) the data protection requirements (i.e. data minimisation); and (c) the technical solutions for data protection by design in the field of eID. The doctrinal research highlighted unlinkability as a key area for data protection by design.

[119] W Lawrence Neuman, *"Social Research Methods: Qualitative and Quantitative Approaches"* (7th, Pearson, 2011) 167.

[120] David Scott, *"Resolving the quantitative–qualitative dilemma: a critical realist approach"* (2007) 30(1) International Journal of Research & Method in Education 3 , 13.

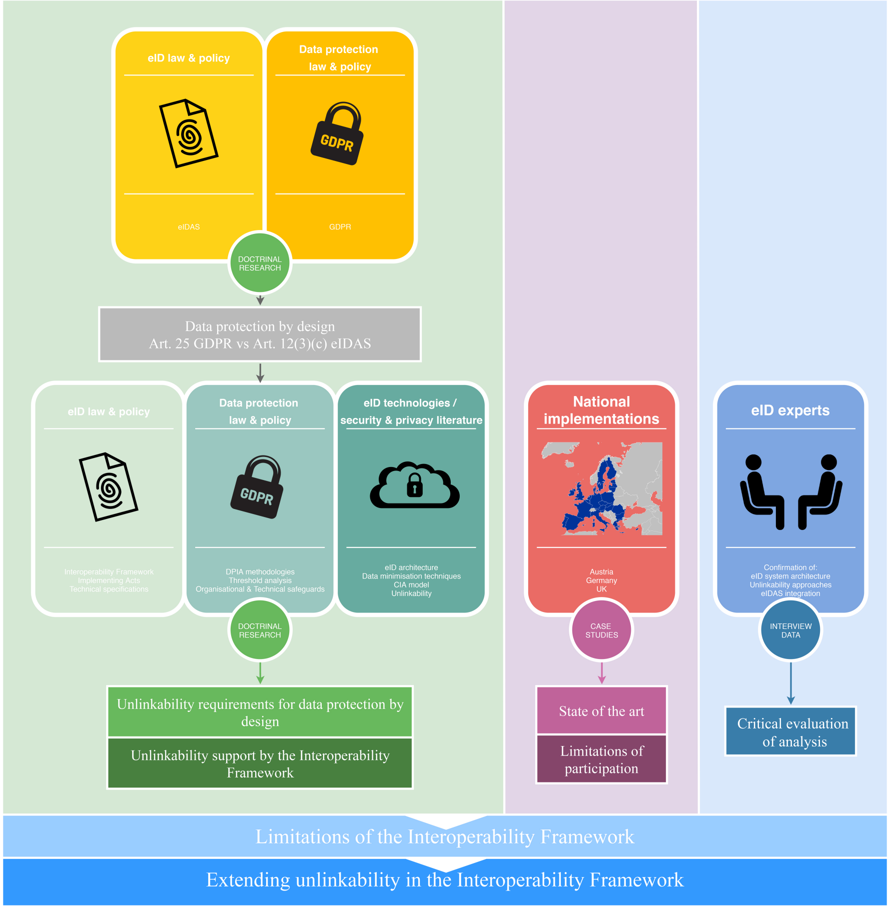

eID law & policy
eIDAS
Data protection law & policy
GDPR
GDPR
DOCTRINAL RESEARCH
Data protection by design
Art. 25 GDPR vs Art. 12(3)(c) eIDAS
eID law & policy
Interoperability Framework
Implementing Acts
Technical specifications
Data protection law & policy
GDPR
DPIA methodologies
Threshold analysis
Organisational & Technical safeguards
eID technologies / security & privacy literature
eID architecture
Data minimisation techniques
CIA model
Unlinkability
DOCTRINAL RESEARCH
Unlinkability requirements for data protection by design
Unlinkability support by the Interoperability Framework
National implementations
Austria
Germany
UK
CASE STUDIES
State of the art
Limitations of participation
eID experts
Confirmation of:
eID system architecture
Unlinkability approaches
eIDAS integration
INTERVIEW DATA
Critical evaluation of analysis
Limitations of the Interoperability Framework
Extending unlinkability in the Interoperability Framework

FIGURE 2.1: Overall research design

However, the practical application of unlinkability could not and should not be fully examined only through desk research, as eID schemes employ different interpretations of what unlinkability is and what level of it is adequate. Further, in an attempt to achieve technological neutrality, high-level policies like eIDAS, the GDPR and second-level EU legislation typically abstain from detailed explanations of how unlinkability can be implemented. Since, therefore, the boundaries between theoretical constructs and practical use were blurred, an empirical investigation of the phenomenon at hand (i.e. unlinkability application) within its real life context was needed.[121] Besides, under the GDPR effective data protection by design relies on the real life context (i.e. *"the state of the art"*). For this purpose, three case studies of national eID schemes were selected.

The case studies selected focused on the eID schemes of Austria, Germany and the UK. The three systems were selected because they represent the higher end of the spectrum in terms of (advertised) data protection by design technology. They each claim to provide federated eID management while guaranteeing a high level of data

[121] Yin (n 114) 13.

protection for their users.[122] However, they each use different architectural and policy models. As a result, looking at all three allowed an examination of schemes with central databases (Austrian ACC), mediating central brokers (Gov.UK Verify) and completely decentralised components (Germany's nPA). Further, the three schemes demonstrate different combinations of public/private eID provision, ranging from completely public (Austria) to public-private (UK) and user-owned (Germany). It was considered, therefore, that these three case studies were capable of providing a complete overview of the modern eID landscape. The three case studies derived the state-of-the-art in data protection by design, with implications for a wider set of national eID systems that move towards that direction (for example, systems in Spain and Portugal)[123] and eIDAS' Interoperability Framework aiming at interconnecting them.

The analysis from the doctrinal research and the case studies were later critically evaluated by a round of expert interviews. The interviews had a triple purpose: firstly, to go beyond the desk research in examining and understanding the role of unlinkability in eID schemes for data minimisation and data protection purposes; secondly, to experience hands-on how unlinkability has been approached in European eID schemes from the experts implementing it; and lastly, to scrutinize the analysis of the limitations that participation in the Interoperability Framework will pose to national eID schemes and investigate the prospects of a practical application of my proposed solution.

The interviews followed a semi-structured format, using an interview guide combining both declarative and open-ended questions. The semi-structured format was selected so that the interviewees would have the opportunity to tailor their answers to the points they considered most relevant. It also permitted the interviewees to raise topics they deemed important. Allowing the experts to deviate from the questions posed was crucial to eliminate any bias introduced by the researcher.

Interviewees were selected through expert sampling, based on their experience in the architectural or policy design of eID schemes. It was decided to consider only experts with experience in European eID schemes, since only EU schemes are within the material scope of eIDAS. However, it was desired to expand beyond the three schemes examined by the case studies to collect data about schemes that were not represented by the case studies. Besides, confirming the state of the art with experts unrelated to the

[122] *See* for the Austrian Citizen Card (ACC) https://www.a-sit.at/de/dokumente_publikationen/flyer/buergerkarte_en.php "...guarantees a high level of data protection and rules out the risk of people shorn off all privacy."; for Germany's nPA https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html "...secure electronic identification is of crucial importance in order to enable trust in electronic services. The German eID is designed to provide this trust."; for UK's Gov.UK Verify https://identityassurance.blog.gov.uk/2014/11/05/protecting-privacy-in-gov-uk-verify/ "The GOV.UK Verify approach is a good starting point for a 'privacy-positive' authentication system, since concepts of anonymity, data minimisation and user control are baked into the underlying technical and commercial models."

[123] For a comparison of the commonalities between EU systems *see* PBLQ, *International Comparison eID Means* (Final Report, 1.0, 2015) ⟨https://www.government.nl/binaries/government/documents/reports/2015/05/13/international-comparison-eid-means/international-comparison-eid-means.pdf⟩ accessed 2 June 2017 19–22.

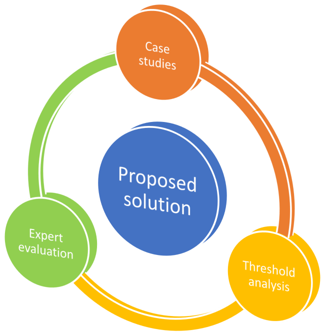


FIGURE 2.2: Triangulation of findings

three schemes was expected to increase the impartiality of the results. In terms of sample size, although a size of around 20 to 30 participants is usually suggested for semi-structured interviews in order to reach saturation,[124] for studies with a high-level of homogeneity, like the field of national eID provision, it has been argued that a much smaller sample is sufficient for meaningful themes and useful interpretations.[125] Interview invitations aimed at two categories of participants: Government officials who shape the goals and design of the related policies of national schemes; and system engineers in charge of the technology and operation of national schemes. A large number of potential participants was approached since it was anticipated that participation rates might be low. Participants were approached through email invitations. The criterion for their inclusion in the sample was only their past or present working experience during the design or deployment of a European national eID scheme. Additional inclusion criteria were purposely not set, in an attempt to eliminate selection bias. Taking into account the tight schedules of practitioners in the field and the time constrains of the research, interviews were conducted with experts from 6 countries, currently representing a third (1/3) of the Member States with notified national schemes. Note that at the time of recruiting only 9 Member States had notified their eID schemes, raising representation to two thirds (2/3). Because of the novelty of the field, this sample size was considered adequate to reach saturation. Data collected from the experts' interviews were thematically analysed to identify common patterns.

The themes that emerged from the interviews expanded on the findings from the doctrinal research and were combined with the state of the art as shown by the case studies. The triangulation of findings (figure 2.2) resulted in a comprehensive analysis of the status and limitations of data protection by design for national eID schemes wishing to participate within eIDAS interoperability framework, before concluding with a practical solution to enhance data protection by design.

[124] Greg Guest, Arwen Bunce, and Laura Johnson, *"How many interviews are enough? An experiment with data saturation and variability"* (2006) 18(1) Field Methods 59 , 61.

[125] The authors seem to propose that in most cases a sample size of 6 would be enough to reach saturation: ibid 78.

2.4 Conclusion

This chapter presented an overview of the methodology followed in this thesis. It explained that because of the subject matter of the research question, and in order to mitigate methodological limitations, a mixed-methods interdisciplinary approach was selected.

The approach comprised of three stages: (a) doctrinal research for the substantive interpretation of the legal rules and the identification of resulting obligations; (b) case-study analysis to examine the current implementation in practice and derive the state of the art; and, (c) in-depth expert interviews to discuss the analyses and evaluate the findings.

The triangulation of methods and findings allowed a holistic examination of the research question. Besides, as argued in chapter 4, a holistic approach is precisely the requirement of data protection by design.

The next chapter will present the legal analysis that was performed to identify the impact of the GDPR on eIDAS. The result of the analysis focused the research question to the level of data protection by design that can be achieved by the Interoperability Framework.

Chapter 3

Combining eIDAS and the GDPR: classification of requirements

Processing of personal data shall be carried out in accordance with Directive 95/46/EC
— eIDAS ART 5(1)

Directive 95/46/EC is repealed with effect from 25 May 2018.
References to the repealed Directive shall be construed as references to this Regulation.
— GDPR ART 94

3.1 Introduction

Processing performed for the purposes of eID by definition involves person identification data – i.e. personal data. eIDAS should be consistent with the data protection framework, which was updated by the GDPR. The goal of this chapter is to examine the impact of the GDPR on eIDAS and determine whether eID under eIDAS and the Interoperability Framework is consistent with the obligations set forth by the GDPR. Such an examination is not a straightforward exercise for two reasons:

First, compliance with the GDPR is conditional upon the specifics of the personal data processing. Assessing the specifics of processing under eIDAS is complex because the eID landscape, as shaped by eIDAS, contains a contradiction. In maintaining a technology-neutral tone, eIDAS high-level rules are open to interpretation; at the same time, its implementing acts lay down architectural requirements for the communication between the eID schemes that in practice create specific architectural choices. The variety of technologies in use for eID by the Member States adds to this complexity.

Second, the relationship between eIDAS and the GDPR can be questioned. In case of a conflict between two legal instruments, priority is given on the basis of norm-conflict and legal interpretation principles.[126] Both eIDAS and the GDPR belong to the same tier in the hierarchy of norms in EU law.[127] Consequently both hold the same legal value and any arising conflicts will have to be resolved by an assessment of their scope, subject matter and time of enforcement.

This chapter addresses these two reasons in three steps: It starts with an overview of eIDAS and the GDPR to define their scope and subject matter. Next, the relationship between eIDAS and the GDPR is discussed, and how norm-conflict principles could resolve potential conflicts. Finally, to determine whether conflicts arise, a classification scheme based on the rationale of the legal provisions, or the *ratio legis*, is used. Obligations from eIDAS and the GDPR are classified against seven thematic categories. The eID obligations of each category are then compared to the data protection obligations to synthesize the complete framework of obligations applicable to eID.

The classification demonstrates that in most areas eIDAS and GDPR obligations complement each other. However, there are some areas of overlap. Because of the relationship between eIDAS and the GDPR, in those areas compliance shall be measured against the stricter set of obligations.

The chapter concludes that in the area of data protection by design compliance can be troublesome. The GDPR intends for data protection by design to be flexible and contextual. eIDAS, on the other hand, with its definition of eID and its additional technical requirements in the implementing acts appears to prescribe horizontal and uniform rules for data protection by design. In order to assess whether eIDAS can satisfy Article 25, there is a need to first examine the exact prescription of data protection by design in the GDPR and second determine the context of the data processing within eIDAS' Interoperability Framework and whether the horizontal rules of eIDAS are adequate. This chapter, therefore, puts forward that eID under eIDAS shall be considered consistent with the GDPR to the degree that the Interoperability Framework can satisfy data protection by design.

The material presented in this chapter has been used in *Deliverable 2.7: State of the art in relation to privacy and data protection requirements.*[128] In section 3.2, an overview of eIDAS is given. Section 3.2.1 presents the mechanism for the mutual recognition of national eID schemes and section 3.2.2 explains the configurations that are possible under

[126] Otherwise called legal maxims, these principles define when a legal rule should take precedence over another because of superiority, subject matter or time of enforcement: see section 3.4.

[127] Regulations, directives and decisions, i.e. legislative acts, are in tier three preceded by the constituent Treaties and Charter of Rights (first tier) and the general principles of law (second tier) and superseded by delegated acts (fourth tier) and lastrly the implementing acts (fifth tier): Paul Craig and Cráinne de Búrca, *"Instruments and the Hierarchy of Norms"* in Paul Craig and Cráinne de Búrca, *EU Law: Text, Cases, and Materials* (6th, Oxford University Press 1 July 2015) 105.

[128] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Marc Sel, *Deliverable 2.7: State of the art in relation to privacy and data protection requirements: Preliminary report* (Ref. Ares(2017)522263 - 31/01/2017, FutureTrust consortium 2017) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_ca38279654cc476fb24ecf5657b8be71.pdf⟩ accessed 25 May 2019 (archived at ⟨https://tinyurl.com/ujsvcwm⟩).

eIDAS. Section 3.3 presents a very high-level overview of the GDPR. Finally, section 3.4 explores the relationship between eIDAS and the GDPR. To assist with this exercise, the classification scheme created is explained in section 3.4.1. The classification is then applied to eIDAS in section 3.4.2 and to the GDPR in section 3.4.3. The results of the classification are then combined in section 3.5.

3.2 Regulation (EU) No 910/2014 (eIDAS)

eIDAS[129] was adopted by the Parliament and the Council on 23 July 2014 and became directly applicable on 1 July 2016. Certain provisions about the electronic identification had already become applicable from 17 September 2014,[130] with the mandatory recognition of notified eID schemes from all Member States kicking in on 29 September 2018.[131] Its purpose is to establish a common legal framework for cross-border transactions by (i) defining minimum interoperability requirements for national eID schemes (Chapter II on *"Electronic Identification"*), (ii) expanding the trust services introduced by Directive 1999/93/EC (eSignature Directive)[132] to include electronic seals, time stamps, certificates for website authentication and electronic documents and delivery, and (iii) laying down rules for use of these trust services in electronic transactions (Chapter III, titled *"Trust Services"*). Compared to the repealed eSignatures Directive, eIDAS introduces two significant changes:

- It is an EU Regulation, and as such it is directly applicable in all Member States without the need for them, as a matter of principle, to transpose its provisions into national law, with a view of ensuring the uniform application of eIDAS.
- While the eSignature Directive dealt only with data authentication (ensuring the message was really sent by the claimed sender), eIDAS includes entity authentication provisions (ensuring that the sender has the claimed identity).[133]

eIDAS applies first and foremost to EU Member States, though as a text with EEA relevance its territorial scope extends to the European Economic Area (EEA) Members

[129] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

[130] ibid art 52(2)(a) mainly about the provisions on notification of eID schemes and co-operation within the Interoperability Framework.

[131] ibid art 52(2)(c).

[132] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [2000] OJ L13/12.

[133] Robert Zuccherato, *"Entity Authentication"* in Henk CA van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US 2011) 420–421.

as well.[134] eIDAS applies to Member States eID schemes that have undergone a (voluntary)[135] notification process,[136] although under Article 1(a) the results of the notification shall be recognised by all other Member States. Only national eID schemes that are used for authentication against public services fall within its scope.[137] eIDAS does not cover services used exclusively within closed schemes as per Article 2(2), e.g. organisations' intranets to manage internal procedures.[138] Besides, *"[o]nly trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation"*, as per Recital 21.

3.2.1 Mutual Recognition of eID Schemes

eIDAS aims to follow a technology-neutral principle-based approach to perform its objectives.[139] Chapter II defines the interoperability framework for national eID schemes. Minimum specifications are not defined in the text, but are included in subsequent implementation acts.[140] Member States that wish to allow their eID schemes to be used across borders need to notify their eID schemes to the Commission.[141]

Notification is not obligatory and can only happen for national schemes (either public sector or private officially recognised by the state) that are used to identify citizens at at least one public service.[142] Member States have the option to notify the Commission that they wish to include their national scheme to the list of Article 9 as long as their scheme is

[134] eIDAS (n 129) was incorporated into the EEA Agreement by a Joint Committee Decision, under Annex XI Electronic Communication, Audiovisual Services and Information Society, on 1 June 2019. The process started on 29 August 2014: http://www.efta.int/eea-lex/32014R0910. The EEA is currently comprised of the EU Member States and Iceland, Liechtenstein and Norway. EEA's role is to extend the fundamental freedoms of the EU internal market (i.e. the free movement of goods, capital, persons and services) to the countries of the EEA (for more *see* Catherine Barnard, *Competence Review: The Internal Market* (Department for Business, Innovation and Skills, 2013) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/226863/bis-13-1064-competence-review-internal-market.pdf⟩ accessed 20 November 2016 (archived at ⟨https://perma.cc/5NV2-EYJ2⟩)). EEA legislation is subject to all primary EU legislation at the time of signing of the EEA Agreement (Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area [1994] OJ L1/3, arts 3(2),6) and to certain secondary legislation with EEA relevance (regulations, directives, decisions) by transposition into national law (EFTA Court, *"The EEA and the EFTA Court: Decentred Integration"* (1st, Hart Publishing 2015) 263–266).

[135] eIDAS (n 129) rec 11: *"Member States should not be obliged to notify their electronic identification schemes to the Commission."*

[136] ibid art 2(1).

[137] ibid art 7(b).

[138] ibid rec 21.

[139] Note that under ibid rec 4 it is stated that *"This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met."*

[140] *See* for example Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1, ANNEX.

[141] eIDAS (n 129) art 9.

[142] ibid arts 7, 9.

eligible for notification. Article 7 sets the conditions for eligibility. The notification process includes a lengthy deliberation where Member States make (non-binding) suggestions on the eID scheme in question.[143] Once a scheme has been included in the list it can benefit from the principle of mutual recognition as per Article 6. Following inclusion in the list of Article 9, mutual recognition is mandatory and thereby automatic when:

> *(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;*
>
> *(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;*
>
> *(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.*

Upon mutual recognition of the notified scheme, all other Member States are obliged to incorporate it into their authentication services.[144]

eIDAS focuses on identification and authentication; it specifies that the goal is *"unique representation"* of a person.[145] Implementing Regulation 2015/1501 (hereinafter Impl Reg 2015/1501) clarifies this further in the design of the Interoperability Framework.[146] Under Impl Reg 2015/1501, persons are uniquely identified by transmission of a minimum dataset, which should include a persistent Unique Identifier.[147] The existence of the Minimum DataSet has been criticised for offering less privacy than what is technically possible.[148] eIDAS further specifies a common reference of *"assurance levels"*,[149] or Levels Of Assurance (LoAs) – different levels of certainty about a user's correct identification)

[143] Note that the Member State is free to disregard all comments and that the Commission has no real power to deny notification of a scheme, unless the application is *obviously* fraudulent or faulty.

[144] ibid art 6(1).

[145] ibid art 3(1); Previous drafts defined the goal as *"unambiguously representing a natural or legal person"*: see European Commission, *"Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Text with EEA relevance)"* COM (2012) 238 final, 19; the adopted version changed the phrasing to *"uniquely representing"*, though it is doubtful that resulted in any material change. Cf. the definition given in text of n 21 omitting the requirement of uniqueness. 'Unique' or 'unambiguous' identification led to the definition of the mandatory 'unique identifier' (n 147).

[146] Impl Reg 2015/1501 (n 140) ANNEX 1 pp 1–6.

[147] *See* ibid art 11(1) and ANNEX I.

[148] Fabio Massacci and Olga Gadyatskaya, *How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results* (White Paper, 2013) ⟨https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=whitepapers:seccord-eidas-whitepaper-2013.pdf⟩ accessed 27 January 2020 (archived at ⟨https://tinyurl.com/vn54l3n⟩) 3.

[149] eIDAS (n 129) art 6(1)(b).

	eIDAS LoA	**STORK 2.0** QAA	Example
level of confidence	N/A	N/A	Anonymous submission of a form.
	N/A	1	Opening an e–mail account. The account only verifies that an email address exists.
	‘Low’	2	Online account with an electricity provider. The account only verifies that it relates to an actual electricity meter.
	‘Substantial’	3	Paying online. The account only verifies (a) the user holds a valid bank card and (b) the bank account associated with the card will be used.
	‘High’	4	Using an ePassport to enter a country. The electronic terminal verifies (a) the credentials relate to a valid identity and (b) the identity belongs to the person presenting the ePassport.

Table 3.1: Mapping between levels of STORK and eIDAS

that notified schemes should adhere to. Using the STORK project as a reference point,[150] eIDAS defines named LoAs, low – substantial – high (table 3.1). Level *“Low”* comprises the baseline, with additional criteria as to the way the schemes perform the person identification and authentication added for levels *“Substantial”* and *“High”*. Definition of the levels comes with the Implementing Regulation 2015/1502,[151] which took into account ISO/IEC 29115 and levels 2, 3 and 4 of the STORK pilot.[152] Under Impl Reg 2015/1502 *“Low”* is assigned when evidence are *“assumed”* to be valid, *“Substantial”* after validation of the evidence and *“High”* after biometric validation. eIDAS stipulates that Member States are free to deny access to their electronic services if the service requires a higher LoA than provided by the foreign eID scheme.[153]

[150] STORK defined 4 assurance levels, with 1 being *“no assurance”* and 4 *“high assurance”* B Hulsebosch, G Lenzini, and H Eertink, *D2.3 – Quality authenticator scheme* (STORK deliverable, 3 March, 2009) ⟨https://joinup.ec.europa.eu/sites/default/files/document/2014-12/STORK%20Deliverable%20D2.3%20-%20Quality%20authenticator%20scheme.pdf⟩ accessed 29 July 2015 (archived at ⟨https://perma.cc/R5SH-DQG3⟩) 17–18.

[151] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/7, ANNEX 2 pp 7–20 [hereinafter Impl Reg 2015/1502].

[152] According to ibid rec 4 *“the Large-Scale Pilot STORK, including specifications developed by it, and the definitions and concepts in ISO/IEC 29115 should be taken into the utmost account”*. STORK defined 4 assurance levels with 1 being *“no assurance”* and 4 *“high assurance”*: Hulsebosch, Lenzini, and Eertink (n 150) 17.

[153] eIDAS (n 129) art 6(1)(c).

3.2.2 Possible Configurations of Notified eID Schemes

Notified schemes are expected to interoperate inside an (eIDAS) Interoperability Framework. Anticipating that notified schemes will differ in architecture, the eIDAS Task Force produced Impl Reg 2015/1501. Impl Reg 2015/1501 recitals 2 and 3 point at two options for deployment: notified schemes can either be deployed as redirection servers (proxies) or as individual instances (middleware).

In a proxy configuration, the notifying Member State (sending Member State) operates an eIDAS node domestically relaying authentication requests and authentication assertions[154] between the Service Providers of the foreign Member State (receiving Member State) and the national eID scheme, i.e. the Service Providers send a request to the eIDAS node in the sending Member State. The eIDAS node gathers user input (the use of the eID token) and relays the request to the national eID scheme. The scheme of the sending Member State performs the identification and then sends the authentication assertion – i.e. the verified identification – back to eIDAS node which then relays it to the Service Provider of the receiving Member State.[155] In other words, the processing for the purposes of identification and authentication happens by operators at the sending Member State.

If the deployment is through a middleware, the sending Member State provides the middleware (in the form of an eIDAS node) to the receiving Member State. The middleware is operated by operators at the receiving Member State.[156] In this case the Service Providers request an identification or authentication to the eIDAS node (residing in the receiving Member State) which gathers the user's eID token and performs the authentication. In this case, processing for identification and authentication is performed at the receiving Member State.

Regardless of choice, the proxy or middleware will relay information to the national eID scheme of the receiving Member State through interoperability software (the 'eIDAS node').[157] A choice on deployment of the interoperability software is given as well. Receiving Member States can install the software centrally, so that all Service Provider requests go through the same instance of the software. Obviously this works better in

[154] An authentication assertion is the product of an authentication request sent by an Identity Provider and *"used by the [Service Provider] to validate the user's access rights to the protected resource."*OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview* (Committee Draft, 02, 2008) ⟨http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html⟩ accessed 19 January 2020 (archived at ⟨http://archive.is/V8Qb3⟩) s 3.2.

[155] eIDAS Technical Sub-group, *eIDAS – Interoperability Architecture* (v1.00, 2015) ⟨https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/82797006/eidas_interoperability_architecture_v1.00.pdf⟩ accessed 22 June 2019 (archived at ⟨https://tinyurl.com/vmao3rp⟩) 4.

[156] ibid 4.

[157] European Commission, *eIDAS-Node National IdP and SP Integration Guide* (v1.4.1, 2018) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82772096/eIDAS-Node%20National%20IdP%20and%20SP%20Integration%20Guide%20v1.4.1.pdf?version=2&modificationDate=1554820110372&api=v2⟩ accessed 20 June 2018 (archived at ⟨https://tinyurl.com/yx5ta8px⟩) 7.

architectures with a centralised element, such as a central hub. Or, the Member State can choose to install an instance of the software at every individual Service Provider, if communication with a central element is absent or needs to be avoided.

All communication between the different components is facilitated by the Security Assertion Markup Language (SAML) 2.0 protocol.[158] A (simplified) representation of all possible configurations can be found in figure 3.1.[159]

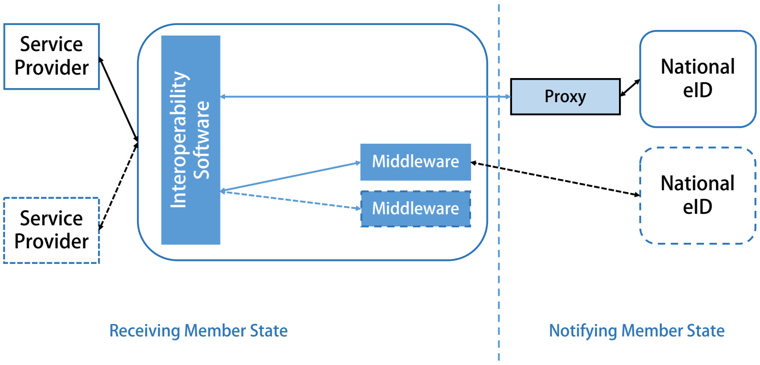


FIGURE 3.1: Configuration options for interoperable schemes

3.3 Regulation (EU) 2016/679 (the GDPR)

eIDAS makes express reference to Directive 95/46/EC[160] via its Article 5(1): *"Processing of personal data shall be carried out in accordance with Directive 95/46/EC."* By definition, all *"person identification data"*,[161] i.e. the identifiers contained within the Minimum DataSet, are personal data. When these attributes are contained in the SAML metadata, the latter become personal data as well. In principle, metadata in the SAML exchanges that do not relate to a natural person will not be considered personal data. For example, the metadata referring to the organisation that operates the eIDAS node[162] will not fall within the scope of data protection legislation. However, should the organization include

[158] Scott Cantor and others, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0* (OASIS Standard, 15 March, 2005) ⟨http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf⟩ accessed 27 February 2017; implying, therefore, that since communication happens through web browser requests, the more components are involved the slower the whole process becomes.

[159] Derived from eIDAS Technical Sub-group, *eIDAS – Interoperability Architecture* (n 155).

[160] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31.

[161] eIDAS (n 129) art 3(3).

[162] Contained in the ⟨md:Organization⟩ element, at least the elements ⟨md:OrganizationName⟩, ⟨md:OrganizationDisplayName⟩, and ⟨md:OrganizationURL⟩: eIDAS Technical Sub-group, *eIDAS SAML Message Format* (v 1.1.2, 2016) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_message_format_v1.0.pdf?version=1&modificationDate=1497252920416&api=v2⟩ accessed 4 November 2019 (archived at ⟨https://tinyurl.com/y6u2qnds⟩) para 2.1.1.

contact information for support and for a technical contact metadata as advised,[163] this information will of course have to be processed according to data protection legislation.

On 27 April 2016 the Commission adopted the GDPR,[164] which entered into force on 24 May 2016 and substituted Dir 95/46/EC on 25 May 2018. The GDPR updated the EU data protection framework, strengthening the protection of individuals' rights.[165] Being a Regulation, the GDPR is directly applicable, except when it allows Member States to adopt more specific rules.[166] Contrary to Dir 95/46/EC, therefore, transpositions into domestic law should not create delays or divergences between Member States[167] and consequently the GDPR has the effect of reducing the margin of manoeuvre of Member States in the field of data protection law.

In order for the GDPR to apply, conditions relating to both its material and its territorial scope should be met:

- The GDPR's material scope relates only to information that are considered as *"personal data"*. Under GDPR Article 4(1) personal data is *"any information relating to an identified or identifiable natural person"*.

[163] *"*SAML *metadata* SHOULD *contain both a* `⟨md:ContactPerson⟩` *element with a* `contactType` *value of 'support' and a* `⟨md:ContactPerson⟩` *element with a* `contactType` *value of 'technical'. The* `⟨md:ContactPerson⟩` *elements* SHOULD *contain at least one* `⟨md:EmailAddress⟩`*."* ibid para 2.1.1.

[164] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[165] See Paul de Hert and Vagelis Papakonstantinou, *"The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals"* (2012) 28(2) Computer Law & Security Review 130 DOI: http://dx.doi.org/10.1016/j.clsr.2012.01.011 for a break down of the most important effects on individuals and data controllers.

[166] Note that the GDPR allows Member States to determine specific conditions for certain data processing activities: *see* for example GDPR (n 164) art 35(1)(4) about the appointment of a Data Protection Officer beside the three reasons provided, ibid art 82 on data processing in employment, ibid art 84 on processing by controllers subject to professional secrecy, ibid art 87 on the processing of national identification numbers. *See* also Cedric Burton and others, *"The Final European Union General Data Protection Regulation"* (2016) 15 BNA Privacy & Security Law Report 153 , s 13. Although during the 'Trilogue' negotiation that led up to the final text the EU Parliament proposed minimum standards for these discretions of Member States (*see* for example EU Parliament: Committee on Employment and Social Affairs, *"Draft Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* (C7-0025/2012 – 2012/0011(COD), 8 November) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), that proposal did not make it to the final text. It remains to be seen, therefore, if the leeway offered to Member States will lead to fragmentation of the data protection rules between states (for example the UK ICO notes that the discretion offered in GDPR (n 164) art 82 might lead to a mandatory appointment of Data Protection Officers in Germany but not in the UK: Information Commissioner, ICO analysis of the Council of the European Union text of the General Data Protection Regulation (2016) ⟨https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf⟩ accessed 18 October 2016 7).

[167] Peter Hustinx, *"EU Data Protection Law - Current State and Future Perspectives"* (Ethical Dimensions of Data Protection and Privacy, 9 September 2014, Centre for Ethics, University of Tartu / Data Protection Inspectorate, Tallinn, Estonia) ⟨https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf⟩ accessed 23 November 2016 5.

- The GDPR's territorial scope, under GDPR Article 3, covers cases where either the data controller or the data processor (or both) are established[168] in the EU, even if the processing is actually taking place elsewhere; or, when the data controller or processor are established elsewhere but they process personal data of data subjects in the Union, if either *"the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;"*[169] or *"to the monitoring of their behaviour as far as their behaviour takes place within the Union".*[170]

Evidently the GDPR will apply in all cases where the processing involves personal data of data subjects located in the EU or the processing happens in EU territory.

3.4 The Relationship between eIDAS and the GDPR

As mentioned, eIDAS is primarily an instrument to establish the mutual recognition of eID schemes across the EU Member States. However, acknowledging that eID will inevitably involve processing of personal data, eIDAS calls upon Dir 95/46/EC to ensure any processing will be compliant with data protection regulations. eIDAS, in other words, recognises that data protection obligations co-exist to an extend with the requirements set forth for eID schemes. A key question, therefore, is to assess the relationship between the two instruments and determine whether eIDAS' requirements should be expanded by obligations and rights set forth by the GDPR, as well as decide which rule will take precedence in areas of overlap.

The GDPR pursues two high-level aims:

1. To ensure natural persons' *"right to the protection of personal data"*[171] and especially by secure electronic exchanges.[172]

[168] An *"establishment"* is defined as any *"effective and real exercise of activity through stable arrangements"* regardless of the *"legal form of such arrangements"*: GDPR (n 164) rec 22; *see* also Judgement of 4 July 1985, *Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, Case C-168/84, EU:C:1985:299, para 18 where the Court decided that for an establishment is required that *"both human and technical resources necessary for the provision of particular services are permanently available"*; Judgement of 13 May 2014, *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, EU:C:2014:317, paras 47–60 where the Court held that undertakings of a controller (in this instance a search engine) should be regarded an extension of the controller's *"establishment"* insofar as they perform processing of personal data *"in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State,"* (at para 57) which in this case involved advertising space among search results; and Judgement of 28 July 2016, *Verein für Konsumenteninformation v Amazon EU Sàrl*, Case C-191/15, EU:C:2016:612, para 77 where the court affirmed that, as set in Weltimmo (Judgement of 1 November 2015, *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, EU:C:2015:639), the stability of the arrangement and the effective exercise of activities are criteria to determine the extent of an establishment.

[169] GDPR (n 164) rec 80.

[170] ibid.

[171] ibid art 1(2).

[172] ibid rec 6: *"Technology [...] should further facilitate the free flow of personal data [...] while ensuring a high level of the protection of personal data."*

2. To ensure *"[t]he free movement of personal data within the Union"*[173] in particular in a cross-border context.[174]

These two aims are shared with eIDAS, in respect to eID:

1. On one hand eIDAS seeks to create *"a common foundation for secure electronic interaction between citizens, businesses and public authorities"*;[175]
2. on the other *"[o]ne of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means"*.[176]

At the same time, eIDAS recognises that eID services have to perform personal data processing for the needs of electronic identification. Recital 11 explains the relationship between eID services and lawful data processing:

> *This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council. In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online.*

Further, Article 5(1) eIDAS establishes that *"[p]rocessing of personal data shall be carried out in accordance with Directive 95/46/EC"*, which was the governing data protection instrument when eIDAS came into force.[177]

However, eIDAS does not go as far as to reproduce the language to be found in ePrivacy Directive.[178] Article 1(2) of ePrivacy Directive states that: *"The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1."* In other words, ePrivacy Directive was enacted with a clear view that it would act as a *lex specialis* to Dir 95/46/EC, prevailing over the latter when processing was performed within the electronic communication sector. This special relationship is recognised also by the GDPR Article 95:

[173] ibid art 1(3).
[174] ibid rec 5: *"The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data."*
[175] eIDAS (n 129) rec 2.
[176] ibid rec 12.
[177] Another example is further along ibid rec 11 in relation to trust services (which are outside the scope of this thesis): *"[R]equirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies."* It seems therefore that eIDAS and Dir 95/46/EC were initially conceived as complementary.
[178] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

> *This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.*[179]

Whether the same approach shall apply to the relationship of the GDPR to other legal instruments has not yet been addressed by neither the EDPB and the courts, and should therefore be assessed on a case by case basis. During the trilogue negotiations, a proposal to amend GDPR Article 95 (Article 89 in the draft proposal) and offer a general rule for norm-conflict resolution. This proposal read as follows: *"Each of the provisions of this Regulation shall apply in so far as there are no specific provisions with the same objective in other Union legislation."*[180] The proposed recital that complemented the amendment illustrated the *lex specialis* principle: *"in accordance with the principle of lex specialis, this Regulation should apply only in so far as there are no specific provisions with the same objective, nature or effect in other existing Union legislation [...] or in future rules of Union legislation."*[181] The proposal did not, however, make it into the final text of the GDPR.

In absence of a general norm-conflict rule, the relationship of the GDPR with other EU legislation will need to be assessed on a case-by-case basis. Legal theory has established three main principles of resolving conflicts when legal instruments may lead to incompatible legal effects. These are encapsulated by three legal maxims:[182] (i) *lex superior*,[183] where priority is given to the rule originating from the higher authority; (ii) *lex specialis*,[184] where priority is given to the more specific rule; and, (iii) *lex posterior*,[185] where priority is given to the rule that was enacted last.

[179] The WP29 discusses this interplay between the two instruments in light of the forthcoming ePrivacy Regulation that will update the ePrivacy Directive in Article 29 Data Protection Working Party, *"Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)"* WP 240, 4; the European Data Protection Board further clarifies in EDPB, *"Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities"* Opinion 5/2019, 14–15.

[180] The Director General, *Annex to Reply from Information Society and Media Directorate General (INFSO) on CIS-Net* (Brussels, INFSO B1/RB Ares (2011), 2011) 17. The proposal was inspired by Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 Setting Out the Requirements for Accreditation and Market Surveillance Relating to the Marketing of Products and Repealing Regulation (EEC) No 339/93 [2008] OJ L218/30, art 15(2) and was envisaged to *"recapitulate[e] the lex specialis principle"* so that *"the relationship between the Regulation and all other Union legislation is clarified once for all, regardless of the final wording of the Regulation."*

[181] The Director General (n 180) 17.

[182] An example of the use of all three legal maxims by the CJEU can be seen in *France v Parliament* where the Court had to prioritise the conflicting norms between Protocol No 6 and art 314 TFEU: see Judgement of 2 November 2018, *France v Parliament (Exercice du pouvoir budgétaire)*, Case C-73/17, EU:C:2018:787, para 42.

[183] *Lex superior derogat legi inferior.*

[184] *Lex specialis derogat lex generali.*

[185] *Lex posterior derogat (legi) priori.*

Applying the three principles to the relationship between eIDAS and the GDPR, *lex superior* cannot in principle provide a satisfactory solution. In contrast to Dir 95/46/EC, which had to be implemented by national law at Member State level, both the GDPR and eIDAS belong to the same tier hierarchically (i.e. they hold the same legal value).

However, data protection, in contrast to eID, has been recognised as a fundamental EU right.[186] Note that, as explained above, eIDAS had already taken a position as to a potential precedence of any Member State implementations of data protection through its Article 5(1). And, the GDPR is *lex posterior* to Dir 95/46/EC, made clear by GDPR Article 94(2).[187] It would seem, thus, that if the GDPR and eIDAS obligations ever diverge, the GDPR will have to prevail.

The precedence of the GDPR over eIDAS where personal data are concerned can be further illustrated through the principle of *lex specialis/lex generalis.* In general, a *lex specialis* is a legal rule that contains more specific provisions over a more general rule, and as such takes priority over the general rule. When special rules are laid down in a set, meant to override a counterpart of general rules, we have a 'self-contained regime'.[188] I.e. 'self-contained regimes' are considered a strong form of *lex specialis*: *"'systems' or 'subsystems' of rules that cover some particular problem differently from the way it would be covered under general law."*[189] 'Self-contained regimes' override the general law in the matters they regulate.

If eIDAS were to be considered a 'self-contained regime' meant to override the GDPR, data processing for the purpose of eID would only have to comply with the obligations set forth by eIDAS. However, even though eIDAS only targets eID[190] and can therefore appear sectorial in comparison with the GDPR, its subject matter does not target only personal data exchanges. Data protection legislation has a different domain of application to eIDAS: The GDPR targets different type of services (data controllers and processors),

[186] Art 16(1) TFEU. *See* GDPR (n 164) rec 12: *"The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."*

[187] *"References to the repealed Directive shall be construed as references to this Regulation."* ibid art 94(2).

[188] Originating from the field of International Law, the term was first coined in *Case of the SS "Wimbledon"* (*U.K. v. Japan*) [1923] PCIJ Rep Series A No 1, para 32. It has since been used extensively in the interpretation of International Law: see Bruno Simma and Dirk Pulkowski, *"Of Planets and the Universe: Self-contained Regimes in International Law"* (2006) 17(3) The European Journal of International Law 483 DOI: 10.1093/ejil/chl015, 490–494. Besides, the CJEU has recognised EU law as a 'self-contained regime' in several cases: see Judgement of 13 November 1964, *Commission of the European Economic Community v Grand Duchy of Luxembourg and Kingdom of Belgium*, Joined Cases 90/63 and 91-63, EU:C:1964:80 (Dairy Products) p 631; Judgement of 15 July 1964, *Flaminio Costa v Ente Nazionale Energia Elettrica (Enel)*, Case 6-64, EU:C:1964:66, p 593; Judgement of 3 August 2008, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, Joined Cases C-402/05 P and C-415/05 P, EU:C:2008:461, p 317.

[189] Martti Koskenniemi, *FRAGMENTATION OF INTERNATIONAL LAW: DIFFICULTIES ARISING FROM THE DIVERSIFICATION AND EXPANSION OF INTERNATIONAL LAW: Report of the Study Group of the International Law Commission* (International Law Commission, 58th session, General Assembly, A/CN.4/L.682, 2006) 68.

[190] and Trust Services.

whereas eIDAS has a narrower scope of only Identity Providers; i.e. it has a different *rationae personae*. The GDPR also targets different types of data exchanges (personal data instead of authentication data – which, apart from the personal data in the eID token, also include data on the LoA, the origin and target public services and relevant metadata);[191] i.e. different *rationae materiae*. It would be difficult, therefore, to argue that eIDAS consists in a 'self-contained regime', i.e. a complete set of rules which would replace in the field of eID the requirements set forth by the GDPR.

Instead, the following observations should be made:

- First, eIDAS contains specific rules for the regulation of eID;
- Second, eIDAS accepts that processing of eID data contains processing of personal data (the person identification data of the eID token);
- Third, eIDAS contains provisions that expressly refer to Dir 95/46/EC, such as Article 5(1);
- Fourth, since eID data contain personal data within the meaning of the GDPR, the latter remains applicable to such data.

By analogy to the interpretation of the CJEU,[192] it should be considered that eIDAS provides a limited set of rules on the regulation of eID (specifically on the interoperation of eID). In this limited set, there are gaps – in this case concerning data protection rules. eIDAS recognises the existence of personal data processing (for example, by explicitly calling eID data *"person identification data"*;[193] by advising for data minimisation)[194] but stays silent about its regulation, referring instead to the EU data protection framework.[195] These gaps must be filled by the application of general rules: in this case, the horizontal obligation created by the GDPR.

Accordingly, it must be considered that eIDAS is not meant to derogate from the general framework to be found in data protection legislation and shall instead be interpreted in harmony with it. Consequently, eIDAS and the GDPR must be conceived as two distinct, but equally applicable, layers of requirements:

- eIDAS comprises a layer of requirements specifically tailored for eID.
- The GDPR comprises a layer of requirements specifically targeting the processing of personal data.

[191] Impl Reg 2015/1501 (n 140) arts 8, 9.

[192] See e.g. Judgement of 19 June 2003, *The Queen, on the application of Mayer Parry Recycling Ltd, v Environment Agency and Secretary of State for the Environment, Transport and the Regions, and Corus (UK) Ltd and Allied Steel and Wire Ltd (ASW)*, Case C-444/00, EU:C:2003:356, paras 52–57; Judgement of 5 November 2014, *Adib Mayaleh v Council of the European Union*, Joined Cases T-307/12 and T-408/13, EU:T:2014:926, paras 198–199.

[193] eIDAS (n 129) art 3(3).

[194] ibid rec 11.

[195] See also the rationale of the EDPB for the relationship between the PSD2 and the GDPR in Letter from Andrea Jelinek on behalf of the European Data Protection Board to Sophie in't Veld MEP (5 July 2018) ⟨https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf⟩ accessed 3 January 2020 (archived at ⟨https://tinyurl.com/yxxawats⟩) 2.

For processing for the purposes of eID, the obligations set forth in eIDAS will apply. When, however, within eID processing of personal data is at stake the GDPR shall prevail over eIDAS.

Their parallel application signifies that in cases where eIDAS mandates the processing of personal data, that processing must be compared against the obligations set forth by the GDPR. Identifying where personal data processing takes place is complex for two reasons: first, because eIDAS is supplemented by a set of Implementing Acts that further extend and particularise its requirements; second, because the adequate protection of personal data will be defined through a relative approach in relation to the processing undertaken for the purposes of eID, as demonstrated in the *Breyer* case.[196] In order to identify the areas of overlap between eIDAS and the GDPR, and examine potential zones of conflict, a classification scheme was created based on the *ratio legis*.

3.4.1 Devising a Classification Based on *Ratio Legis*

Since eIDAS targets eID and trust services and the GDPR data controllers and processors, it was important to distinguish which of their respective requirements apply to eID schemes. Doctrinal research was used to screen legislation and case law and discover the scope and aim behind the legal formulations.[197] The synthesis was used to form a classification scheme of legal requirements applicable to eID schemes. Each requirement was expanded and analysed according to its *ratio legis*. *Ratio legis* refers to the underlying reason or purpose that a specific norm, rule or tribunal decision aims to serve.[198] The aim was to identify the intended purpose of the requirements set forth by eIDAS and the GDPR as they would apply in an eID scheme. *Ratio legis* allowed to create thematic categories of the requirements according to their content. In a similar approach to content analysis,[199] a coding frame was created with labels that summarised the purpose of the corresponding theme (figure 3.2).

Generally speaking, the *ratio legis* of eID requirements can be classified into 6 categories:

[196] Judgement of 19 October 2014, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, EU:C:2016:779, para 62.

[197] Nigel Duncan and Terry Hutchinson, *"Defining and describing what we do: Doctrinal legal research"* (2012) 17(1) Deakin Law Review 83 , 101–105.

[198] *Ratio legis* is a valuable instrument in legal scholarship, as it is used to interpret the intent behind the letter of the law. For a definition of '*ratio legis*' and its role in legal reasoning, *see* in general María José Falcón y Tella, *"Case law in Roman, Anglosaxon and continental law"* (Martinus Nijhoff Publishers 2011); Robert Brandom, *"Between saying and doing: Towards an analytic pragmatism"* (Oxford University Press 2008); Aharon Barak, *"Purposive interpretation in law"* (Princeton University Press 2007); Robert Brandom, *"Making It Explicit. Reasoning, Representing, and Discursive Commitment"* (Harvard University Press 1994).

[199] Lisa Webley, *"Qualitative Approaches to Empirical Legal Research"* in Peter Cane and Herbert M Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2012) 938.

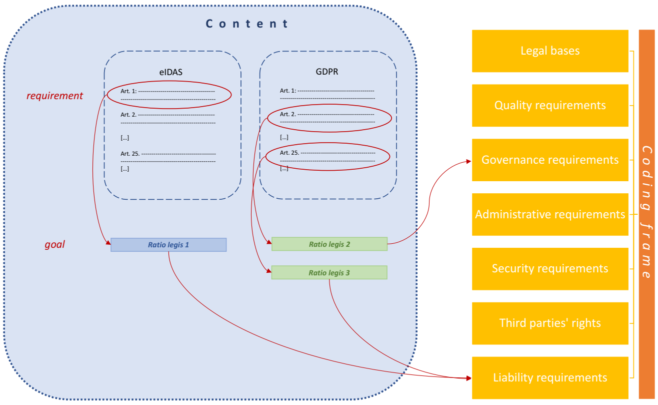


FIGURE 3.2: Context analysis based on ratio legis

(i) QUALITY requirements that place quality constraints on the way operations shall be conducted, including the processing of data, necessary for the purposes of identification and authentication (for eID schemes) or creation, verification, validation and preservation of the products of trust services (for trust services), to the exclusion of legal bases and security requirements.

(ii) GOVERNANCE requirements, relating to *"the processes of interaction and decision-making among the actors involved"*[200] in the provision of eID and trust services to end users. These requirements therefore relate to the number and roles of actors involved in the process of service provisions to end users.

(iii) ADMINISTRATIVE requirements, which captures requirements relating to the internal administration and management of eID providers and their members of staff. They cover for example obligations in relation to record keeping, up to date termination plans and the operation of databases for certificates.[201]

(iv) SECURITY requirements relating to organisational and technical measures eID providers have to put in place in order to ensure the security of their services, including *"the trustworthy cross-border mutual recognition of electronic identification means"* within the meaning of eIDAS.[202]

[200] *"the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions."*Marc Hufty, *"Investigating Policy Processes: The Governance Analytical Framework (GAF)"* in Urs Wiesmann and Hans Hurni (eds), *Research for Sustainable Development: Foundations, Experiences, and Perspectives* (Geographica Bernensia 2011) 405; Rene Kemp, Saeed Parto, and Robert B Gibson, *"Governance for Sustainable Development: Moving from Theory to Practice"* (2005) 8(1/2) Int J Sustainable Development 12 , 17: *"Governance structures organise negotiation processes, determine objectives, influence motivations, set standards, perform allocation functions, monitor compliance, impose penalties, initiate and/or reduce conflict, and resolve disputes among actors"*; Adrian Smith, Andy Stirling, and Frans Berkhout, *"The governance of sustainable socio-technical transitions"* (2005) 34(10) Research Policy 1491 , 1498: *"[Governance] involves interaction between actors in networks".*

[201] Note that one duty or right could have several dimensions, e.g. a duty to conduct audits could be classified under both governance and administration.

[202] eIDAS (n 129) rec 19.

(v) Liability requirements, capturing requirements relating to the identification of the party liable in case of damage, allocation of liability share as well as allocation of the burden of proof. The question is then whether these requirements should be considered as the counterpart of an implicit right to compensation granted to third parties.

(vi) Data Protection, a set of requirements that encapsulate the general data protection obligations. This can be broken down further into

   (i) Legal bases, a set of requirements relevant for the GDPR and covering the list of grounds capable of justifying specific personal data processing activities. The presence of such a set of requirements can be explained by the fact that the GDPR sets common principles for all sectors. With this said, there is an argument that eIDAS could be conceived in conjunction with its implementing acts as a legal basis of its own in some cases, e.g. when it provides for a minimum dataset to be transmitted.[203]

   (ii) Third parties' rights, relating to obligations imposed on providers that directly benefit third parties, who are then entitled to expect from providers a specific performance and thereby assert rights against these providers. These include for example rights to information, to the benefit of relying parties against Identity Providers, or to the benefit of data subjects against data controllers.

This classification scheme has been applied to eIDAS and the GDPR, with sets of requirements derived for eID schemes. Following is the classification of the requirements under eIDAS.

3.4.2 Classification of eIDAS Requirements

eIDAS recognises that identification of citizens is a sovereign matter of Member States.[204] Consequently, eIDAS establishes rules to allow diverse eID schemes to interoperate. To this end, eIDAS provides for the creation of a pan-European 'Interoperability Framework'.

The purposes of eID schemes under eIDAS are identification (*"'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"*)[205]

[203] Impl Reg 2015/1501 (n 140) ANNEX..

[204] This is perhaps due to the variety of national eID architectures deployed in the Member States. Initially this led to the proposal of separate instruments for legislation of trust services and eIDs (cf Key actions 3 and 16 in European Commission, *"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe"* (Communication) COM/2010/0245 f/2); in the end both were addressed under eIDAS but as opposed to the harmonisation in trust services, eID remained under the control of Member States (*see* eIDAS (n 129) rec 13) with provisions for a mutual recognition of the different national schemes.

[205] ibid art 3(1).

and authentication, although authentication is defined as *"an electronic process that enables the electronic identification of a natural or legal person".*[206] In practice this thus means that an eID means should be created with the use of a person's identification data, which will then be used for authentication purposes in the context of relationships with other online services.

In other words, while eID schemes are meant to enable electronic identification, eID means issued under a notified scheme should perform authentication. A three-tier process to achieve electronic identification is provided by Article 8, which identifies three LoAs: Low, Substantial and High. The technical specifications of LoAs are given in Impl Reg 2015/1502.[207] The quality constraints will thus vary depending upon the level of assurance adopted. Quality constraints also include conditions for eligibility as per Article 7 and in particular the obligation to ensure availability of authentication online, the obligation to ensure that the eID uniquely identifies the person it is issued for,[208] as well as interoperability requirements such as the obligation to transmit the Minimum DataSet to identify natural and legal persons.[209]

All notified schemes shall be interoperable as per Article 12(1). Towards that end eIDAS sets out requirements for the interoperability framework as such, which has to be technology neutral, adhere to EU and international standards, facilitate privacy-by-design and comply with data protection rules, include a mapping of the associated national LoA and rules on governance and administration.[210]

Article 9 provides for a series of notification steps to be performed by the notifying Member States. The Commission is responsible for defining the circumstances, formats and procedures of notifications. Article 9 thus provides for both governance and administrative requirements.

Article 10 provides for obligations relating to security breaches and mitigation measures to be put in place by notifying Member States, in particular notification obligations. Article 10(1) reads as follows:

> *Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.*

[206] eIDAS (n 129) art 3(5).
[207] Impl Reg 2015/1502 (n 151).
[208] eIDAS (n 129) art 7(d): *"[T]he notifying Member State ensures that the person identification data uniquely representing the person in question is attributed…".*
[209] Impl Reg 2015/1501 (n 140) ANNEX..
[210] eIDAS (n 129) art 12.

Article 11 caters for liability rules and thereby allocation of liability shares and burden of proof. Member States with notified schemes are liable for the non-performance of two obligations: to ensure availability of authentication online and to ensure that the person identification data uniquely representing the person in question is attributed in compliance with appropriate standards.[211] The eID means issuer shall be liable for the non-performance of the obligation to ensure that the eID means is attributed to the person in question in compliance with appropriate standards and the party operating the authentication procedure shall be liable for the non-performance of the obligation to ensure the correct operation of the authentication.[212] These provisions are without prejudice to already existing national liability rules.[213]

Going further, one question is whether Article 11 therefore indirectly grants to third parties a right to compensation in cases in which damage is caused intentionally or negligently to any natural or legal person. As Article 11 does not expressly specify the type of remedy to be awarded in case of liability, it is doubtful whether Article 11 could be interpreted in this sense.

The final text of the Regulation shows an attempt to balance liability between all parties involved in an eID scheme. Earlier drafts included stricter liability provisions for the Member State,[214] which had led some commentators to question whether the Member States' would assume responsibility for other parties' compliance with eIDAS.[215]

Generally speaking, eIDAS requirements can be grouped together, according to the classification analysed above, into six groups — or sets — of requirements, *(i)* quality, *(ii)* governance, *(iii)* administrative, *(iv)* security, *(v)* liability and *(vi)* data protection. An overview of each group of requirements, pursuing a specific objective within a complex relational scheme, is given below and summarized in table 3.2.

(i) Quality: While eID schemes are meant to make electronic identification possible[216] electronic identification means of natural and legal persons falling under a notified identification scheme should perform an authentication function[217] Nevertheless eIDAS

[211] ibid art 11, referring to ibid arts 7(d), 7(f).

[212] ibid arts 11(2), 11(3).

[213] ibid arts 11(4), 11(5).

[214] COM (2012) 238 final (n 145) 6(1), on responsibility of unambiguous attribution of eIDs lacks the phrase *"at the time the electronic identification means under that scheme is issued"* (eIDAS (n 129) arts 11, 7(c)), pertaining constant liability of the member state throughout the use of an eID. *Mutatis mutandis* between ibid art 7(f) and COM (2012) 238 final (n 145) 6(1)(d), whose wording required Member States guaranteeing availability of the scheme *"at any time"* and did not allow Member States to limit their liability with T&C towards private sector relying parties.

[215] *See*, for example, Jos Dumortier and Niels Vandezande, *"Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market"* [2012] ICRI Research Paper 9 ⟨http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152583⟩ accessed 25 December 2016 , 7.

[216] *"the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"*: eIDAS (n 129) art 3(1).

[217] Authentication under eIDAS means *"an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed"*: ibid art 3(5).

distinguishes between different levels of assurance and in this sense eligible schemes should *(a)* comply with at least one of the three LoA that should be *(b)* equal or higher than the LoA of the service they are attempting to access.[218] They should be *(c)* available online and *(d)* transmit the Minimum DataSet to identify natural and legal persons.[219] The interoperability framework shall *(e)* be technology neutral[220] and *(f)* allow for Privacy-by-design principles, with a specific mention to the data minimisation principle.[221] *(g)* Data protection compliance of all components is also a requirement.[222] Requirements *(f)* and *(g)* should be conflated with the general obligation *(vi)* that applies to all processing (and not only on the Interoperability Framework).

(ii) GOVERNANCE: Eligible schemes should (*a*) identify citizens against at least one public sector service and be either (*b*) issued by the Member State, (*c*) issued by a third party under mandate from the Member State or (*d*) issued under mandate of a third party but recognised by the Member State.[223] They should also be (*e*) included in the Notification list of Article 9 and (*f*) be supervised by a national body.

(iii) ADMINISTRATIVE: Schemes should (*a*) have a published description of its operation, have set (*b*) liability regimes, (*c*) arrangements for suspension and revocation procedures, (*d*) rules of procedure and (*e*) dispute resolution mechanisms, (*f*) public T&C of use for non-public-sector services and (*g*) have appointed a data registration manager.[224]

(iv) SECURITY: Eligible schemes should adhere to (*a*) EU and international standards, have set (*b*) suspension and revocation procedures (also under section 3.4.2) and (*c*) withdrawal procedures in case of a security breach that lasts more than 3 months.[225]

(v) LIABILITY: Aside from (*a*) national rules of liability, the Member State is liable (*b*) for the appropriate attribution of the eIDs and (*c*) the availability of authentication online. (*d*) The party issuing the eIDs is liable for the appropriate attribution of an eID to a person and (*e*) the operator of the eID scheme is liable for a failure to ensure the correct operation of the identification process.[226]

[218] eIDAS (n 129) arts 8, 6(1), 6(2); compliance with LoAs ensures the levels of certainty any given identification should produce.

[219] Impl Reg 2015/1501 (n 140) ANNEX..

[220] The first drafts of the Regulation required Member States to operate schemes that could guarantee that no extra hardware or software would be necessary in order for other Member States to access them. This wording has been toned down in the final text after objections from some Member States, so that eIDAS (n 129) art 7(f) now reads: *"Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication". See* Colette Cuijpers and Jessica Schroers, *"eIDAS as guideline for the development of a pan European eID framework in FutureID"* (2014) 2014(237) Open Identity Summit 23 , 23–38.

[221] With services required to request and process only data strictly necessary for each individual authentication: eIDAS (n 129) rec 11 *"processing of only those identification data that are adequate, relevant and not excessive"* and ibid art 12 [the Interoperability Framework] *"facilitates the implementation of the principle of privacy by design"*.

[222] ibid art 12(3)(d).

[223] ibid arts 7(a), 7(d).

[224] ibid art 12.

[225] ibid arts 10, 12.

[226] ibid art 11.

(vi) DATA PROTECTION: Finally, under its 'General Provisions' eIDAS introduces a general obligation for all parties to comply with data protection. Mentions to specific data protection obligations happens only in relation to the Interoperability Framework, as explained in *(i)(f)* and *(i)(g)*.

	quality	governance	administrative	security	liability	data protection
requirements	**Eligibility conditions** (Art. 7) for eID schemes and in particular: - The schemes can be used to access (at least) one public service (*Art. 7(b)*) - Schemes should support (at least) one of LoA (*Arts. 7(c), 8(1)*) - Person identification data uniquely representing the person appropriately attributed (*Art. 7(d)*) - eID means appropriately attributed - Availability of authentication online (*Art. 7(f)*) **Interoperability** requirements for eID schemes and in particular: - Notified schemes shall be interoperable. (*Art. 12(1)*) - The schemes transmit the Minimum DataSet (*Art. 12(3)(d)*) The **framework** (and not the schemes) in particular shall: - aim to be technology neutral and not discriminate among different national technological solutions (*Art. 12(3)(a)*) - facilitate Privacy by Design (*Art. 12(3)(c)*) - comply with data protection law (*Art. 12(3)(d)*	Notified schemes are at a minimum recognised by the **notifying Member State** (*Art. 7(a)*) Notified schemes can involve **3 parties**: the Member State, the party issuing the eID means and the party operating the authentication procedure (*Art. 3*) National schemes are notified to the **EC** (*Art. 9*) The schemes are included in the Notification List published by the **EC** (*Arts. 6(1)(a), 9*) The schemes are under a **supervisory regime** (*Art. 9(1)(b)*) The interoperability framework is distinct from the schemes (*Art. 12*)	A **description of the schemes** has been submitted (*Art. 9(1)(a)*) A **description of the liability regime(s)** of the schemes has been submitted (*Art. 9(1)(b)*) Information of the entities that **manage registration data** for the schemes (*Art. 9(1)(d)*) **Suspension or revocation** procedures for the schemes have been arranged (*Art. 9(1)(g)*) **No disproportionate technical requirements** imposed on Service Providers (*Art. 7(f)*) Requirements concerning the **content of the interoperability framework** (*Art. 12(4)*)	Immediate **suspension and revocation** of compromised components of schemes (*Art. 10(1)*) Obligation of **information** of other Member States and the EC when breach remedied (*Art. 10(2)*) If compromised for more than 3 months, **withdrawal** of the scheme (*Art. 10(3)*) The EC shall **modify the list of notified schemes** when withdrawal of the notified scheme. (*Art. 10(3)*) Interoperability framework complies with **EU & International standards** (*Art. 12(3)(b)*)	Member State liable for a failure to ensure (negligently or intentionally) that the **person identification data uniquely representing the person** in question is appropriately attributed (*Art. 11(1)*) Member state liable for a failure to ensure (negligently or intentionally) the **availability of authentication** online (*Art. 11(1)*) The party issuing the eID means liable for a failure to ensure (negligently or intentionally) that the **eID is appropriately attributed** to the person (*Art. 11(2)*) The party operating the authentication procedure liable for a failure to ensure (negligently or intentionally) the **correct operation of the authentication** (*Art. 11(3)*)	Processing of personal data shall be carried out **in accordance with data protection regulations** (*Art. 5(1)*)

TABLE 3.2: eID schemes and framework requirements

3.4.3 Classification of GDPR Requirements

The GDPR can be described via the same categories of requirements as eIDAS, with the addition of an extra category of legal bases, which are needed to justify the processing before quality requirements can apply.

The GDPR governs processing of personal data. 'Personal data' refers to *"any information relating to an identified or identifiable natural person ('data subject');"*[227] legal entities are excluded from the definition. Even though the definition in large mirrors the one found in Dir 95/46/EC, the GDPR adds to the explicitly stated examples and introduces the notion of 'singling out'.[228] In Recital 30, online identifiers are explicitly mentioned as (potential) personal data.[229] Personal data that have been processed in such a manner that they can no longer be attributed to a specific data subject without the use of additional information are introduced as a special category of data, data that has undergone pseudonymisation.[230]

A 'data controller' is *"a natural or legal person, public authority, agency or other body which [...] determines the purposes and means of the processing of personal data."*[231] Processing refers to *"any operation or set of operations which is performed upon personal data"* without an exhaustive list of cases, which has led to a wide interpretation of the term.[232] The criterion of who determines the purposes and means of processing seems to define which entities should be considered as controllers. WP29 considers that control

[227] GDPR (n 164) art 4(1).

[228] ibid rec 26: "...account should be taken of all the means reasonably likely to be used, such as singling out..."; in analysing the means likely reasonably to be used the WP29 includes the cost of conducting the identification; the intended purpose of the processing; the way the processing is structured; the advantage expected by the data controller; the interests of the data subject; and any risk of organisational and technical failure. The likely reasonably test appears to be a relativistic or contextual one — *see* Khaled El Emam and Cecilia Álvarez, *"A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques"* (2015) 5(1) International Data Privacy Law 73 DOI: 10.1093/idpl/ipu033; Sophie Stalla-Bourdillon and Alison Knight, *"Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data"* (2016) Forthcoming Wisconsin International Law Journal 1 ⟨http://eprints.soton.ac.uk/id/eprint/400388⟩ accessed 11 January 2017 .

[229] The inclusion of online identifiers in the definition of personal data should not necessarily condemn the contextual approach followed by the CJEU in its recent case law. *See Breyer* (n 196) paras 45–49 where the Court decided that dynamic IP addresses can constitute personal data and Judgement of 17 July 2015, *YS v Minister voor Immigratie, Integratie en Asiel; Minister voor Immigratie, Integratie en Asiel v M and another*, Joined Cases C-141/12 and C-372/12, EU:C:2014:2081, paras 38–48 where the Court decided that a legal analysis does not constitute personal data; cf *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311, [2015] All ER (D) 307 [115(ii)] where the UK Court of Appeal held that browser-generated information can be considered personal data in as far as they reveal a unique IP address, a browsing history and a rough geographic location, as this information sufficiently 'individuates' an individual against others; *see* also Stalla-Bourdillon and Knight (n 228) fn 70.

[230] GDPR (n 164) art 4(5).

[231] ibid art 4(7).

[232] Judgement of 6 November 2003, *Criminal proceedings against Bodil Lindqvist*, Case C-101/01, EU:C:2003:596, paras 24–27 where Dir 95/46/EC (n 160) art 3(1) was interpreted to include mere uploading on an Internet page; *Bodil Lindqvist* (n 232) para 41 stating that Dir 95/46/EC applies to non-economic activities as trying to distinguish between economic and non-economic activities would make *"the field of application of the Directive particularly unsure and uncertain"* – same also in Judgement of 20 May 2003, *Österreichischer Rundfunk and Others*, Joined Cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paras 39–47.

can stem from both explicit legal competence (under national or EU law) or form implicit competence from roles that imply a certain responsibility or from factual influence.[233] Therefore, data controllers play a key role in controlling if, why and how personal data are processed. In some cases, though, an entity will be regarded as a controller even if it lacks factual control, like when regarded as such by Union or Member State law.[234]

A 'data processor' is any "natural or legal person [...] which processes personal data on behalf of the controller."[235] A processor is thus a separate entity from the controller, processing data on behalf of the controller after being instructed to do so. The processor has to comply with a certain number of obligations and in particular security obligations as per Article 32 of the GDPR. The GDPR burdens the status of data processors by additional obligations, such as requirements to maintain adequate documentation,[236] implement security measures,[237] carry out impact assessments,[238] appoint a Data Protection Officer (DPO)[239] and cooperate with national supervisory authorities (DPAs).[240] A written data processing agreement should be in place between the processor and the controller,[241] meeting the requirements of the GDPR. Failure to meet these requirements can subject the processor to administrative sanctions[242] who may also have to face compensation claims from individuals.[243]

A 'data subject' is any natural person whose personal data are processed by a controller or its processors.[244] Data subjects are granted specific rights by the GDPR, e.g. right to information,[245] right to access data,[246] right to alter the data collected,[247] right to object to further processing[248] or profiling[249] or withdraw their consent, right to receive a copy of the data and offer them to a different controller,[250] or right to ask for their deletion (*"right to be forgotten"*)[251] as well as an explicit right to compensation as per Article 83.

[233] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 2010) 10–12; factual influence was used for example in its position for cloud client as controllers and the cloud providers as data processors: Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing* (WP 196, 2012) 7–8.

[234] GDPR (n 164) art 4(7): *"where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"*.

[235] ibid art 4(8).

[236] ibid art 30.

[237] ibid art 32.

[238] ibid art 32.

[239] ibid art 37.

[240] ibid art 31.

[241] ibid art 28.

[242] ibid art 83.

[243] ibid art 79.

[244] ibid art 4(1).

[245] ibid arts 12–14.

[246] ibid art 15.

[247] ibid art 16.

[248] ibid art 18.

[249] ibid art 22.

[250] ibid art 20.

[251] ibid art 17.

Processing of personal data requires a legitimate ground or legal basis under Article 6.[252] An important legal basis is consent. Consent has to by (a) unambiguous, (b) specific, (c) informed and (d) freely given.[253] This is particularly important for online services, as it means that any consent to processing shall be given through opt-in rather than opt-out principles.[254] It is disputed whether that consent will need to be explicit or it can be implied.[255] Blanket consent is prohibited and the scope and consequences of all processing activities should be made clear to the data subject for consent to be valid.[256] Notably Recital 43 of the GDPR adds that if there is *"clear imbalance between the data subject and the controller, in particular where the controller is a public authority"* consent is not an appropriate legal basis. And as per Article 6(4), in order to determine whether consent was freely given, account should be taken of whether data unnecessary for the performance of the contract was processed. Another legal basis is when the processing happens as part of fulfilment of a contract to which the data subject is a party.[257] Many existing relationships between data subjects and their national eID authorities, eID means issuers and/or eID authenticators as well as their relationships with electronic Service Providers are/could be covered by contracts. As far as legal bases are concerned, it is worth mentioning the 'legitimate interest' of the data controller, except *"where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child,"* which is to be found in Article 6(f). Importantly, Recital 47 specifies that *"the reasonable expectations of data subjects based on their relationship with the controller"* should be taken into account to assess the legitimacy of the data controller's interest.

The GDPR sets a set of quality requirements that data controllers should comply with: Generally speaking, personal data shall be *"processed lawfully, fairly and in a transparent manner in relation to the data subject"*[258] under the lawfulness, fairness and transparency principles.

[252] As stated in Opinion of 26 January 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16, EU:C:2017:43, para 38 *"the default rule underpinning that directive is that personal data should, in general, not be processed"*.

[253] GDPR (n 164) arts 6(1), 4(11), 7.

[254] Article 29 Data Protection Working Party, *The Future of Privacy* (WP 168, 2009) paras 65–68; Eoin Carolan, *"The continuing problems with online consent under the EU's emerging data protection principles"* (2016) 32(3) Computer Law & Security Review 462 DOI: http://dx.doi.org/10.1016/j.clsr.2016.02.004, 467.

[255] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definiton of consent* (WP 187, 2011) 24.

[256] Bart W Schermer, Bart Custers, and Simone van der Hof, *"The crisis of consent: how stronger legal protection may lead to weaker consent in data protection"* (2014) 16(2) Ethics and Information Technology 171 DOI: 10.1007/s10676-014-9343-8, 176 noting that users suffer from an information overload which prohibits them from making active, informed choices; Antoinette Rouvroy and Yves Poullet, *"The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy"* in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) DOI: 10.1007/978-1-4020-9498-9_2 89–90 noting that consent must be respectful of the fundamental rights of the data subject.

[257] GDPR (n 164) art 6(2).

[258] ibid art 5(1).

The purpose limitation principle requires that personal data can only be processed for specific purposes and cannot be further processed in a manner incompatible with these specific purposes.[259] The data controller has an obligation to make known the purposes for which the data are acquired.[260] Note that this principle is not a prohibition of further processing. However, there does not seem to be consensus on the implications of that principle. While WP29 seems to require a new legal basis for each act of processing,[261] including acts of further processing, this view does not seem to be shared by everyone.[262] When deciding on incompatibility, the relationship between the original purposes and the further processing should be considered, along with the context and the nature of the collected data, the reasonable expectations of the data subjects and the safeguards of the controller to ensure fair processing.[263] These considerations have been incorporated into Article 6(3a) of the GDPR.[264]

The quantity of data gathered should be proportionate to the relevant purpose and should be adequate, relevant and limited to only what is necessary.[265] The data minimisation principle is considered to be a sub-part of the data-protection-by-design and by-default principles.[266] It provides that only the data necessary for the specific purpose determined before the actual processing should be processed.[267]

Data should be kept accurate and, where necessary, up to date.[268] This is the accuracy principle. Personal data should only be kept for no longer than is necessary for the

[259] GDPR (n 164) art 5(2); Peter Carey, *"Data protection: a practical guide to UK and EU law"* (4th, Oxford University Press 2015) 59.

[260] *"collected for **specified** [...] purposes"* [emphasis added] GDPR (n 164) art 5(2). *See* also Carey (n 259) 58–59.

[261] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (WP 203, 2013) 12.

[262] European Union Agency for Fundamental Rights, *"Handbook on European data protection law"* (2nd, Publications Office of the European Union 2014) 69.

[263] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (n 261) 13.

[264] During the drafting phase the Council had proposed that controllers should be able to further process data for incompatible purposes. This was met with resistance from Member States and EU bodies and was not included in the final version: Burton and others (n 166) s 1.

[265] GDPR (n 164) art 5(1)(c); Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (WP 223, 2014) 6.

[266] Also present under eIDAS (n 129) art 1. Cf Laura German and others, *Consolidated report on the socio-economic basis for trust and trustworthiness* (D2.5, OPTET – OPerational Trustworthiness Enabling Technologies 2015) ⟨http://www.optet.eu/wp-content/uploads/deliverables/OPTET_WP2_D2.5_Consolidated_report_on_the_socio-economic_basis_for_trust_and_trustworthiness_v1.0.pdf⟩ accessed 10 October 2015 (archived at ⟨http://archive.fo/sqgts⟩) 36–38 about the limited scope of the included PbyD principles in the GDPR (namely data protection by design and data minimisation) that overlooks a number of other values and issues (such as intellectual property).

[267] In eID schemes, for example, the minimum requirements are given by Impl Reg 2015/1501 (n 140) under the Minimum Dataset.

[268] GDPR (n 164) art 5(1)(d); this is an obligation of the controller. In Carey (n 259) 62–64 it is suggested that controllers can comply with the principle as long as they can demonstrate they have given data subjects enough controls to monitor the accuracy of their data and are acting upon notification of any inaccuracies.

purposes for which the personal data is processed.[269] Compliance with this requirement would, for example, require deletion, destruction or anonymization of data that is no longer necessary.[270] This requirement is already in place in several national eID schemes.[271] This is the storage limitation principle.

Moreover, appropriate technical and organisational measures must be implemented to ensure protection against unauthorised or unlawful processing, accidental loss, destruction or damage.[272] This confidentiality and integrity principle is substantiated by Article 32 of the GDPR, which provides in its first paragraph that:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) The pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing schemes and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

Therefore, both controllers and processors have to comply with the integrity and confidentiality principle. The GDPR also introduces[273] its own data breach notification obligations.[274] As the language of Article 33 of the GDPR is not exactly the same as the language of Article 19 of eIDAS it is worth reproducing it:

[269] GDPR (n 164) art 5(1)(e); the principle should be read in light of the *"right to be forgotten"* ((ibid art 17 and recs 65–68)) in order to ensure the data subject's consent is still valid in case consent was the legal basis of the processing: Luiz Costa, *"Data Protection Law, Processes and Freedoms"* in *Virtuality and Capabilities in a World of Ambient Intelligence: New Challenges to Privacy and Data Protection* (Springer International Publishing 2016) DOI: 10.1007/978-3-319-39198-4_6.

[270] Carey (n 259) 64.

[271] For example, data used to issue eIDs in Germany under the nPA scheme, where any facial photographs or fingerprints must be destroyed after issuance of the eID: Gilad L Rosner, *"Identity management policy and unlinkability: a comparative case study of the US and Germany"* (PhD thesis, University of Nottingham 2014) 189.

[272] GDPR (n 164) art 5(1)(f).

[273] Following recommendations that have been around for some time: Article 29 Data Protection Working Party, *Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (WP 184, 2011).

[274] GDPR (n 164) art 33; the GDPR opted to elevate this as a general data controller obligation following in the steps of the ePrivacy directive: de Hert and Papakonstantinou, *"The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals"* (n 165) s 11.

> *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

At the same time, Article 34 paragraph 1 provides that: *"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."* Exceptions to this rule exist however: communication with data subjects is not required if at least one condition is met as per Article 34(3).

Controllers are required to keep a record of all data breaches and permit audits by the supervisory authority.[275] Generally speaking, controllers are required to *"maintain a record of processing activities under [their] responsibility."*[276] The content of these records is regulated in further detail.[277]

Furthermore, Article 35 imposes upon the controller the obligation to undertake a data-protection impact assessment before initiating the processing *"[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing."* Where the impact assessment indicates that the absence of measures would result in a high risk, the controller shall consult the supervisor authority prior to processing.[278]

Parenthetically, the GDPR clarifies in detail the tasks of supervisory authorities. The DPAs of each Member State typically have the role of supervisory authorities; Member States can assign additional independent public bodies as supervisory authorities.[279] The tasks of supervisory authorities include obligations to (a) monitor and enforce the application of the GDPR; (b) promote awareness of the risks, rules, safeguards and rights pertaining to personal data; (c) advise national and governmental institutions on the application of the GDPR; (d) handle claims brought by data subjects or their representatives; (e) establish requirements for Impact Assessments, Codes of Conduct, certifications, Model Clauses and Binding Corporate Rules; and (f) keep records of sanctions and enforcement actions.[280] Supervisory authorities have the power to oversee enforcement of the GDPR, investigate breaches and bring legal proceedings where

[275] GDPR (n 164) art 33(5).
[276] ibid art 30(1).
[277] ibid arts 30(1), 30(2).
[278] ibid art 36(1).
[279] ibid art 51(1).
[280] ibid arts 55,57.

necessary.[281] Along with the controllers' obligations for record keeping and auditing of Articles 30, 31 and 33, they could form a separate set of '*monitoring and enforcement*' requirements. This set has been, however, omitted from this analysis since the focus is on the responsibilities of the controllers (and processors).

What is more, the GDPR imposes new governance rules for certain categories of organisations. These organisations are required to appoint a DPO. DPOs must have expert knowledge of data protection law and the role can be outsourced to service providers.[282] Organisations that are part of public authorities, process data that by nature, scope or purposes require regular and systematic monitoring of data subjects on a large scale or whose activities consist of processing sensitive data on a large scale must appoint a DPO.[283]

Finally, as regards liability, the GDPR has its own liability rules and in particular sets as a general principle that *"any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*[284] The controller and processor are therefore jointly liable for the damage suffered by the data subject. In addition, the burden of proof is shifted to the detriment of both the controller and the processor so that *"[a] controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage."*[285] To be sure, data subjects get more than a right to compensation against the controller or processor. They also get a right to lodge a complaint with a supervisory authority as per Article 77, as well as right to an effective remedy against a supervisory authority as per Article 78 of the GDPR. With this said, even though the precise expression *"right to compensation"* is used in the GDPR, it appears that if the controller or processor is able to show that it is not *"in any way responsible for the event giving rise to the damage,"* the data subject will not be able to obtain compensation from this controller or processor.

Interestingly, when full compensation has been paid by the data controller or the processor, one has the right to claim back from the other the amount corresponding to its part of responsibility as per Article 82(5).

To summarise, the requirements of the GDPR can be classified into *(i)* legal bases, *(ii)* quality, *(iii)* governance, *(iv)* administrative, *(v)* security, *(vi)* third parties' rights, and *(vii)* liability requirements as follows:

[281] ibid art 58.

[282] ibid arts 37(5), 37(6).

[283] Cf n 166 about the role of national legislation in appointment of DPOs.

[284] GDPR (n 164) art 82(1).

[285] ibid art 82(3).

(i) Legal bases: At the least one of the following legal bases should apply: *(a)* The data subject has given their consent,[286] or the processing is necessary *(b)* for the performance of a contract[287] or *(c)* for compliance with a legal obligation[288] or *(d)* to protect vital interests of natural persons[289] or *(e)* to exercise official authority or for public interest[290] or *(f)* for legitimate interests of the controller or a third party.[291]

(ii) Quality: Given one (or more) of the legal bases is satisfied, data processing *(a)* should incorporate the principles of Data Protection by Design and by Default;[292] *(b)* should be conducted fairly, lawfully and transparently,[293] only for the pre-defined purposes (*(c)* purpose limitation principle)[294] and only for necessary amount of data (*(d)* data minimisation principle);[295] *(e)* has to be accurate[296] and *(f)* shall preserve the data only for as long as necessary (storage limitation).[297]

(iii) Governance: Data controllers and processors should adhere to certain governance requirements, according to which they should *(a)* be subjected to regular auditing procedures[298] and *(b)* continuous supervision,[299] *(c)* notifying the supervisory authority of data breaches.[300] The supervisory authority shall *(d)* maintain and publish a list of the kind of processing that is subject to data protection impact assessments,[301] and the controller shall *(e)* consult the supervisor prior to processing if a data protection assessment has indicated that the measures the controller has taken are not adequate to mitigate a high risk.[302] Supervisory authorities have an obligation of *(f)* cooperation, assistance and collaboration between them,[303] and *(g)* a consistency mechanism between the EDPB and the Commission is to be set up.[304]

(iv) Administrative: Data controllers need to *(a)* have appropriate technical and organisational measures in place,[305] *(b)* appropriate data protection policies,[306] *(c)* maintain records of their processing activities,[307] *(d)* carry out data protection impact assessments

[286] GDPR (n 164) art 6(1)(a).
[287] ibid art 6(1)(b).
[288] ibid art 6(1)(c).
[289] ibid art 6(1)(d).
[290] ibid art 6(1)(e).
[291] ibid art 6(1)(e).
[292] ibid art 25.
[293] ibid art 5(1)(a).
[294] ibid art 5(1)(b).
[295] ibid art 5(1)(c).
[296] ibid art 5(1)(d).
[297] ibid art 5(1)(e).
[298] ibid art 58(1)(b).
[299] ibid arts 39(1)(b), 54, 57, 58.
[300] ibid art 33.
[301] ibid art 35(4).
[302] ibid art 36.
[303] ibid arts 60–62.
[304] ibid art 63.
[305] ibid arts 24(1), 28(1).
[306] ibid art 24(2).
[307] ibid art 30(1).

when there is a high risk to the rights and freedoms of natural persons,[308] and *(e)* have a designated Data Protection Officer[309] for a series of tasks.[310]

(v) SECURITY: Controllers and processors shall *(a)* conform with the integrity and confidentiality principle,[311] *(b)* notify data breaches to the supervisory authority[312] and *(c)* the data subjects,[313] and *(d)* ensure a level of security appropriate for the risks of processing via technical and organisational measures[314] (also under *(iv)(a)*).

(vi) THIRD PARTIES' RIGHTS: Processing must respect the data subject's right to *(a)* information about the data processing,[315] *(b)* access the data held with the controller or processor,[316] *(c)* rectify said data,[317] *(d)* ask for the erasure of some or all of their data,[318] *(e)* ask for restriction of the processing,[319] *(f)* transfer their data to a different controller or processor ('data portability'),[320] *(g)* object to some or all of the processing[321] *(h)* or to decisions based solely on automated processing of their data,[322] *(i)* ask for compensation,[323] *(j)* file a complaint with the supervisory authority,[324] challenge the decisions of controllers, processors or supervisory authorities and access an *(k)* effective judicial remedy against the controller or processor[325] or *(l)* the supervisory authority.[326]

(vii) LIABILITY: Finally, the GDPR updates the rules on liability of controllers and processors, making them *(a)* jointly liable for data breaches,[327] and *(b)* placing the burden of proof with the controller or processor who have to prove they did not act intentionally or negligently.[328]

[308] ibid art 35.
[309] ibid art 37.
[310] ibid art 39.
[311] ibid art 5(1)(f).
[312] ibid art 33.
[313] ibid art 34.
[314] ibid art 32.
[315] ibid arts 12, 13.
[316] ibid art 15.
[317] ibid art 16.
[318] ibid art 17.
[319] ibid art 18.
[320] ibid art 20.
[321] ibid art 21.
[322] ibid art 21.
[323] ibid art 82.
[324] ibid art 77.
[325] ibid art 79.
[326] ibid art 78.
[327] ibid art 82(4).
[328] ibid art 82(3).

	legal bases	quality	governance	administrative	security	third parties' rights	liability
requirements	**Prior consent** of the data subject (*Art. 6(1)(a)*)	Data-Protection **by Design** and **by Default** (*Art. 25*)	Subject to **supervision** by supervisory authority(-ies) (*Arts. 39(1)(b), 54*) with specific tasks (*Art. 57*) and powers (*Art. 58*)	Appropriate **technical and organisational measures** to be put in place (*Arts. 24(1), Art. 28(1)*)	**Integrity** and **confidentiality** principle (*Art. 5(1)(f)*)	Right to **information** (*Arts. 12, 13*) Right to **access** (*Art. 15*)	Controllers and processor **jointly** liable (*Art. 82(4)*)
	Processing necessary for the **performance of a contract** (*Art 6(1)(b)*)	Processing **fairly**, **lawfully** and **transparently** (*Art. 5(1)(a)*)	Controllers and processors to undergo **regular auditing** (*Art. 58(1)(b)*)	Implementation of appropriate data protection **policies** by the controller (*Art. 24(2)*)	Appropriate **technical and organisational measures** to ensure a level of security appropriate to the risk (*Art. 32*)	Right to **rectification** (*Art. 16*) Right to **erasure** (*Art. 17*)	**Burden of proof** lies with the controller or the processor (*Art. 82(3)*)
	Processing necessary for compliance with **legal obligation** (*Art. 6(1)(c)*)	**Purpose limitation** principle (*Art. 5(1)(b)*)	**Notification** of data breaches to supervisory authorities (*Art. 33*)	Maintenance of **records** of processing activities (*Art. 30(1)*)	**Notification** of data breaches to supervisory authority (*Art. 33*)	Right to **restriction** of processing (*Art. 18*) Right to **data portability** (*Art. 20*)	
	Processing necessary to protect **vital interests** of natural persons (*Art. 6(1)(d)*) Processing necessary for **public interest** or exercise of **official authority** (*Art. 6(1)(e)*)	**Data minimisation** principle (*Art. 5(1)(c)*) **Accuracy** principle (*Art. 5(1)(d)*)	The supervisory authority shall establish and make public a **list of the kind of processing** operations which are subject to the requirement for a **data protection impact assessment** (*Art. 35(4)*)	**Data-protection impact assessment** when a high risk to the rights and freedoms of natural persons (*Art. 35*) Designation of a **Data Protection Officer** (Art. 37) with a series of task (*Art. 39*)	**Notification** of data breaches to data subjects (*Art. 34*)	Right to **object** (*Art. 21*) Right not to be subject to a decision based solely on **automated processing** (*Art. 21*) Right to **compensation** (*Art. 82*)	
	Processing necessary for **legitimate interests** of the controller or third party (*Art. 6(1)(f)*)	**Storage limitation** principle (*Art. 5(1)(e)*)	The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates a high risk in the absence of measures taken by the controller to mitigate the risk. (Art. 36) **Cooperation**, **mutual assistance**, and **collaboration** between lead supervisory authority and other authorities (*Art. 60-62*) **Consistency** mechanism involving the EDP Board and the Commission (*Art. 63*)			Right to lodge a **complaint** with a supervisory authority (*Art. 77*) Right to an **effective judicial remedy** against a supervisory authority (*Art. 78*) Right to an **effective judicial remedy** against a controller or processor (*Art. 79*)	

Table 3.3: GDPR requirements

3.5 Combining the Two Layers of Requirements

While the two layers of requirements aforementioned are meant to be applied in harmony with one another, an overlap can be observed in at least two occasions: the rules around liability and the requirements on data protection by design.[329] For each of these occasions, either the GDPR or eIDAS is more restrictive. Regarding liability requirements, eIDAS appears to provide a stricter allocation of liability by considering specific parties *de facto* responsible depending on their role in the eID process.[330] And, although eIDAS mandates the 'facilitation' of data protection by design, it only contains a general obligation for data minimisation in its (non-binding) recital 11. On the contrary, GDPR Article 25 makes data protection by design conditional upon a series of criteria.

Because, as explained in section 3.4, eIDAS cannot be seen as a 'self-contained regime' it would be difficult to argue that eIDAS would derogate from the GDPR on some specific points by virtue of *lex specialis*. Besides, as a matter of principle it would seem odd to have less restrictive solutions for eID in relation to liability and data protection by design, when these providers and services are conceived as key promoters of trust in the information society to the benefit of EU citizens. Consequently, the question that arises is whether eIDAS can be reconciled with the requirements of the GDPR in the areas of overlap.

Regarding liability requirements, eIDAS and the GDPR can work in parallel. Under the GDPR, an infringement of its obligations that has caused material or immaterial damage results in joint liability of the controllers and the processors involved.[331] Further, the GDPR seems to provide that, by default, the burden of proof shall lie with the data controller or the data processor. This seems to result from paragraphs 2 and 3 of Article 82, which reads as follows:

> *2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.*
>
> *3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.*

[329] Another overlap can be observed in relation to notification obligations, if the classification is expanded to include the Trust Services provisions of eIDAS: eIDAS (n 129) art 19(2) appears both more restrictive and broader than GDPR (n 164) arts 33, 34, in the sense that it sets a stricter deadline of 24 hours (vs. 72 in the GDPR) and is triggered by any security or integrity breach, not just by personal data breaches. However, since the Trust Services are out of the scope of this thesis, this overlap was discarded.

[330] For example, for damage caused because of inaccurate person identification data, the Member State is held responsible (eIDAS (n 129) art 11(1)) whereas for damage caused because the eID means does not represent the correct person, the Identity Provider is responsible (ibid art 11(2)).

[331] GDPR (n 164) art 82(4).

On the other hand, eIDAS Article 11 provides liability rules for three scenarios: Where damage has been caused intentionally or negligently due to wrong attribution of the data uniquely representing a person;[332] or due to non-availability of the online authentication;[333] or due to incorrect operation of the online authentication.[334] Under eIDAS, it is indifferent whether the damage was caused due to a violation of a data protection duty or obligation. In fact, the aim of eIDAS Article 11 seems to be to assign liability to the correct party in the complex operation of online authentication, where frequently multiple parties from eID schemes of different architecture will be involved. As such, eIDAS determines that in the first scenario, the responsible parties are the issuer of the eID means and the Member State endorsing the eID scheme. In the second scenario, the responsible party is the Member State endorsing the eID scheme. And in the third, the responsible party is the operator of the online authentication.[335] It seems, therefore, that eIDAS' attempt is to ease the question of whom a person shall seek remedies from by assigning default responsibility to certain entities. Contrary to eIDAS Article 13 about Trust Service Providers, the provisions on liability in eID do not attempt to reverse the burden of proof.[336] Importantly, eIDAS is silent as to the remedies that can be sought for redress.

Accordingly, it would seem that when damage occurs during an online authentication, remedies should be sought against the responsible party under the eIDAS rules on liability. However, when personal data are at stake and damage has been caused due to a violation of a data protection duty or obligation, the responsible party under eIDAS shall be liable *jointly* with the data processors that were involved in the incident. This would make sense given the precise remedies prescribed by the GDPR, and in particular the right to compensation for data subjects. Given the very broad definition of personal data, it is likely that the GDPR will often complement eIDAS' liability rules.

Satisfaction of the GDPR data protection by design obligations might prove harder. At first glance eIDAS seems to have expected data protection by design to some extent, insofar as its Article 12(3)(c) mandates the *"facilitat[ion]"* of *"privacy by design"*. However, the formulation of GDPR Article 25 introduces contextual factors that ought to be examined in order to determine if the level of data protection afforded by eIDAS is satisfactory. Notably, the Interoperability Framework and its technical standards and specifications

[332] eIDAS (n 129) arts 11(1), 11(2).

[333] ibid art 11(1).

[334] ibid art 11(3).

[335] This is not to say that, as a rule, these parties will always be separate entities. In the case of a national eID scheme, where a governmental body is in charge of issuing the eID means and operating the eID scheme, damage occurred during any of the three scenarios will always result in the liability of the Member State.

[336] Cf eIDAS (n 129) art 13(1) and the difference between qualified and non-qualified providers: *"...The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.*

"The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider."

act as a common denominator for cross border exchanges and do not necessarily mitigate data protection risks in the same way as national eID schemes.

In other words, eIDAS constructs a positive list of attributes that will be processed for the purposes of eID. It further uses the various implementing acts and technical standards to define the measures that will safeguard this list of attributes. This list of attributes is meant to be processed in all cases of eID, i.e. even in cases where not all attributes are necessary. Prior to the GDPR, national laws that expressly defined such lists of attributes on the basis of statutory authorisation were treated as *lex specialis* to the data minimisation principle.[337] However, the GDPR does not provide exceptions from the principles of Article 5. In fact, Article 25 explicitly conditions data protection by design to the satisfaction, among others, of the overarching principles of Article 5. The question, then, becomes whether the definition of a default list of attributes by eIDAS is compatible with the GDPR Article 25.

3.6 Conclusion

As explained, eIDAS comprises of rules and requirements tailored for data processing for the purposes of eID. The GDPR, on the other hand, comprises of rules and requirements targetting the processing of personal data. Even though eIDAS only targets eID, it cannot be considered an instrument with sectorial application to the GDPR as eIDAS' subject matter encompasses processing of all data needed for eID, not just personal data. However, it is recognised by virtue of Article 5(1) that eIDAS cannot derogate from the GDPR framework. Consequently, eIDAS and the GDPR should be viewed as two equally applicable layers of requirements.

To identify any areas of overlap and potential inconsistencies in the parallel application of the two layers, the requirements of eIDAS and the GDPR were divided into seven sets based on their *ratio legis*. The analysis that followed demonstrated that most sets contain requirements that are complimentary to one another. However, an overlap was discovered in the requirements around liability requirements and data protection by design requirements (part of the QUALITY requirements). In those areas eIDAS should be consistent with the GDPR obligations.

With respect to liability rules, eIDAS can be reconciled with the GDPR's allocation of the burden of proof and available remedies for damages occurring from the processing of personal data. However, because of eIDAS' implementing acts and technical specifications, assessing the consistency with the requirement of data protection by design needs further

[337] See, e.g., Mariusz Krzysztofek, *"Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679"* (Wolters Kluwer 2017) s 4.05, citing labour, banking and consumer protection laws.

investigation. The technical specifications and the accompanying implementing acts need to be assessed in light of GDPR Article 25.

The next chapter looks into the principle of data protection by design. It analyses its exact prescription under GDPR Article 25 in order to derive its impact in the field of eID and help determine whether there is a real conflict between GDPR Article 25 and eIDAS 12(3)(c).

Chapter 4

The challenge of data protection by design

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
>
> — GDPR Art 25(1)

4.1 Introduction

As explained in the previous chapter, cross-border eID within the Interoperability Framework shall comply with parallel obligations from eIDAS and the GDPR. At large, the parallel obligations work complementary to each other. However, an overlap between GDPR Article 25 on data protection by design and eIDAS Article 12 on facilitation of privacy by design can be observed. eIDAS Article 12 will eventually need to be expanded to accommodate Article 25 of the GDPR. To understand the implications of such an expansion, though, first the scope and meaning of the ‘by-design’ obligations in the two Articles need to be clarified.

eIDAS does not provide a precise definition of privacy by design in its text. By interpretation of Article 12(3)(c), Article 5(1) and 5(2), and Recital 11 it can be extrapolated that privacy by design should at least relate to the concepts of data minimisation and pseudonymisation. Any additional requirements included in its implementing acts and technical specification may, however, impact upon this prescription.

In contrast, the GDPR defines data protection by design by reference to key concepts of data protection: the data protection principles of Article 5, the rights of the data subjects of Articles 12–23, the purposes of processing of Article 6, the security of processing of Article 32, and the risks to the data subjects of Article 35. It appears, therefore, that data protection by design is formulated in close connection with a plethora of obligations under the GDPR.

The goal of this chapter is to investigate the formulation and substance of GDPR Article 25 and derive the exact prescription of data protection by design. It begins by an analysis of the origins of privacy by design to clarify the substance of the data protection by design obligation. It then explains its evolution into the data protection by design principle.

Privacy by design had been an emerging theme in system engineering since the 1970s that eventually gained traction with the data protection authorities. Comprising a collection of high-level principles and engineering models, privacy by design champions the treatment of privacy as an integral part of system design. It suggests that effective protection must be iterative throughout the life-cycle of a system though a combination of soft (policy) and hard (technology) measures.

The GDPR recognised the importance of privacy by design and incorporated it into the data protection framework. Article 25 importantly termed the principle 'data protection by design' and extended privacy by design to encompass the necessary protections for personal data, namely the controller and processor obligations and the protection of data subject rights. In doing so, the GDPR conditions compliance with data protection by design on the satisfaction of particular criteria. Eventually, adequate satisfaction will depend on a balancing test between the processing and the risks it poses to the data subjects. In other words, data protection by design under the GDPR must be risk-based. In light of this, this chapter concludes that data protection by design requires a parallel reading of the impact assessment requirements of Article 35.

Section 4.2 below presents the evolution of data protection by design from the concept of privacy by design, and section 4.3 details how data protection by design was conceptualised in Article 25 of the GDPR. Of note, the material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness.*[338]

4.2 The Evolution of Data Protection by Design

Data protection by design has its origin in the concept of 'privacy by design'. Privacy by design is a term used to signify that modern system engineering ought to be built in such

[338] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

a way that the privacy of the users is adhered to in the architecture of the system itself, i.e. the technological components. In other words, privacy protections should be built in the system in such a way that the technology itself does not allow privacy breaches. The protections should be introduced from the conception of the system and be present throughout the life-cycle of its operation.[339] This is in contrast to the previous practice, where measures for privacy and security where taken only through soft policy measures. Policy measures under privacy by design are still necessary, but on their own they are considered less effective – *"an afterthought"*.[340]

This reflects concepts that existed in system engineering since the 1970s,[341] but the term is attributed to the Information and Privacy Commissioner of Ontario Ann Cavoukian. Cavoukian proposed the *"Privacy-embedded laws of identity"*,[342] a commentary on the original 7 principles proposed by Kim Cameron,[343] that coincided with the discussions about 'privacy-by-design' and fair trade policies. The main goal around the 'laws of identity' was to ensure that interoperability of identity management systems would not endanger data safety. In simple words, that using the same eID means across multiple services would not make it easier to monitor where the eID means has been used, to aggregate data from its use and to profile the holder of the eID means. The 'laws of identity' mandate that a privacy-embedded system would by design offer the below features:

1. Freedom of choice to the user and personal control to consent where and from whom identification will happen.

2. Well defined frames of identity requirements so as to minimize data disclosure to the bare minimum for each service.

3. Access to data to only those parties authorized to do so.

[339] Ann Cavoukian and Mark Dixon, *Privacy and Security by Design: An Enterprise Architecture Approach* (2013) ⟨https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf⟩ accessed 20 January 2017 (archived at ⟨http://archive.fo/tVTPe⟩) 7–14.

[340] Daniel Le Métayer, *"Privacy by Design: A Formal Framework for the Analysis of Architectural Choices"* (CODASPY '13, ACM 2013) DOI: 10.1145/2435349.2435361 95.

[341] See, for example, Herbert Burkert, *"Privacy-enhancing Technologies: Typology, Critique, Vision"* in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy* (MIT Press 1997); David L Chaum, *"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"* (1981) 24(2) Commun. ACM 84 DOI: 10.1145/358549.358563; David Chaum, Amos Fiat, and Moni Naor, *"Untraceable Electronic Cash"* (Shafi Goldwasser ed, Springer New York 1990) DOI: 10.1007/0-387-34799-2_25; Tom Wright and Peter Hustinx, *Privacy-Enhancing Technologies: The Path to Anonymity* (Volume 1, 184530, 1995) ⟨http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf⟩ accessed 23 May 2019 (archived at ⟨http://archive.fo/0p30U⟩).

[342] Ann Cavoukian, *7 Laws of Identity the Case for Privacy-Embedded Laws of Identity in the Digital Age* (White Paper, 2006) ⟨http://www.ontla.on.ca/library/repository/mon/15000/267376.pdf⟩ accessed 11 June 2019 (archived at ⟨http://archive.fo/IaE5H⟩).

[343] Kim Cameron, *"The Laws Of Identity"* (*Identity Blog*, 5 November 2005) ⟨http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf⟩ accessed 11 June 2015 (archived at ⟨http://archive.fo/LSkNo⟩).

4. Support for multiple types of identities so as to allow the user to select what data to store in each and where to use each one.

5. Interoperability of services and segregation of providers so as to minimize cross-linking and profiling attempts.

6. Despite the underlying technologies, the system must offer a uniform experience to the end users.

7. The system must thoroughly inform the users about their choices and their consequences.[344]

These principles were used to propose what has been called 'user-centric' models of eID management: Enhancements that put the user at the centre, regardless of the architectural design of the system. Alongside, a discourse of 'privacy-enhancing technologies' was created, i.e. a set of systems that promote respect for privacy.[345] Privacy enhancing technologies stand for *"a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."*[346] They were later endorsed by the European Commission *"in particular where personal data is processed through ICT networks."*[347] Privacy enhancing technologies enhance the traditional 'CIA' model of cyber security (confidentiality, integrity and availability)[348] with four additional components:

> *Anonymity (and pseudonymity)*: Anonymity of a subject in a system means that an attacker cannot sufficiently identify the subject within a set of subjects. Pseudonymity, in this sense, is a means of anonymising datasets. Anonymity often relates closely to *selective disclosure*, the ability of eID management systems to transmit only some of the identifiers contained in an eID means (so, for example, only the anonymised ones).[349]
>
> *Unlinkability*: The inability of an attacker to know if any two points of interest in a system are related (for example, an eID means with its owner). Edge unlinkability, a subset of unlinkability, focuses on the components of the system: when a component

[344] Cavoukian (n 342) 2-19.

[345] Lee A Bygrave, *"Hardwiring Privacy"* in Roger Brownsword, Eloise Scotford, and Karen Yeung, *The Oxford Handbook of the Law and Regulation of Technology* (Roger Brownsword, Eloise Scotford, and Karen Yeung eds, Oxford University Press 2017) 4–5.

[346] John Borking, Paul Verhaar, and Gilles W van Blarkom, *"PET"* in John Borking and others, *Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents* (PISA Consortium 2003) DOI: 10.13140/2.1.4888.7688 33.

[347] European Commission, *"On Promoting Data Protection by Privacy Enhancing Technologies (PETs)"* (Communication) COM(2007) 228 final, 4.

[348] Matt Bishop, *"Introduction to Computer Security"* (Addison-Wesley Professional 2004) 2–4;International Organization for Standardization, *Information technology – Security techniques – Code of practice for information security controls* (ISO/IEC 27002:2013, 2013).

> at one end of the system cannot link an action to any other component of the system, edge unlinkability is served.[350]
>
> *Undetectability*: from the point of an attacker refers to their inability to locate a particular point of interest in the scheme (for example, if a service exists within the system).[351]
>
> *Unobservability*: Unobservability refers to the undetectability of scheme components from all other components inside the scheme (for example, a service within the system does not know who the other services of the system are).[352]

Note, however, that even though privacy enhancing technologies are a useful tool in privacy engineering, they present a limited scope of data protection as data confidentiality,[353] which is not enough to cover other aspects of protection like data protection as accountability of the controller or data protection as control by the user. In this sense, the concept of 'data protection by design' explained below is an enrichment of privacy by design.

The privacy by design ideas soon found their way to the agendas of data protection authorities. In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a resolution recognising *"Privacy by Design as an essential component of fundamental privacy protection"*[354] that should be applied *"as a holistic concept"*.[355] Around the same time, WP29 was also promoting privacy by design as an additional principle of data protection.[356] Eventually, the privacy by design philosophy was introduced in the reform of the EU data protection legislation with the Article 25 of the GDPR.

4.3 Data Protection by Design under the GDPR

Article 25(1) of the GDPR reads as follows:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying*

[352] Andreas Pfitzmann and Marit Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology* (v0.33, 2010) ⟨https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.doc⟩ accessed 12 June 2015 (archived at ⟨https://tinyurl.com/ycshm2ey⟩) 9-12.

[352] ibid 12-13.

[352] ibid 16.

[352] ibid 16.

[353] Michael Veale, Reuben Binns, and Jef Ausloos, *"When data protection by design and data subject rights clash"* (2018) 8(2) International Data Privacy Law 105 DOI: 10.1093/idpl/ipy002, 107.

[354] 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (2010) ⟨https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf⟩ accessed 15 June 2019 (archived at ⟨http://archive.fo/fmxxB⟩) 2.

[355] ibid 1.

[356] Article 29 Data Protection Working Party, *The Future of Privacy* (WP 168, 2009) para 8.

> *likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

Article 25 builds on the *"responsibility of the controller"*[357] to impose a duty on data controllers to put in place technical and organisational measures in order to (a) implement data protection principles (first and foremost the principles of GDPR Article 5), and (b) to safeguard the rights of the data subjects. It should not be considered, however, that the thrust of Article 25 is limited to the principles of Article 5. When WP29 recommended privacy by design for inclusion in the EU data protection framework, it noted that the principle encompassed under its umbrella an evaluation of several related concepts: the processing of no personal data at all or as few personal data as possible; the support for effective control by the data subjects so that they are free to exercise their rights; the adequacy of the information, help and interfaces provided to the data subjects; the disclosure of the data only to authorised entities; the accessibility and accuracy of the data; the segregation of data, processes and purposes in systems that run in a multi-user environment.[358] To assume that Article 25 has a narrow scope only around the principles of Article 5 would be to disregard the close relationship between the data protection principles and the obligations and rights set forth by the rest of the GDPR provisions.

Article 25 is formulated similarly to Article 32 on adequate security.[359] However, unlike Article 32, the obligations of Article 25 need to be adhered to from the design phase (*"the determination of the means"*) all throughout the life-cycle of the processing.

The formulation of the principle in the GDPR as *"data protection by design"* clearly focuses on privacy as implied in data protection. Narrowing down the scope of privacy has been considered necessary in order to avoid the multi-layered concept of privacy which makes it hard to pin down and, therefore, satisfy.[360]

[357] GDPR (n 164) art 24.

[358] In WP29's terms: *"Data Minimization"*, *"Controllability"*, *"Transparency"*, *"Data Confidentiality"*, *"Data Quality"*, *"Use Limitation"* Article 29 Data Protection Working Party, *The Future of Privacy* (n 356) para 53; in respect to data subjects rights, in fact, WP29 conceptualises *"functionality [that] should be included facilitating the data subjects' right to revoke consent, with subsequent data erasure in all servers involved (including proxies and mirroring)."* ibid para 14.

[359] Lee A Bygrave, *"Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements"* (2017) 4(2) Oslo Law Review 105 , 114.

[360] Mireille Hildebrandt and Laura Tielemans, *"Data protection by design and technology neutral law"* (2013) 29(5) Computer Law & Security Review 509 DOI: https://doi.org/10.1016/j.clsr.2013.07.004, 517; Kieron OHara, *"The Seven Veils of Privacy"* (2016) 20(2) IEEE Internet Computing 86 DOI: 10.1109/MIC.2016.34, 87–89.

Data protection by design applies, first and foremost, to data controllers.[361] Data processors are indirectly captured by GDPR Article 25, at least in as much as data controllers *"shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures"*.[362] Interestingly Recital 78 notes that

> *producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*

This is therefore a mere encouragement,[363] even though, as Bygrave notes, system manufacturers and engineers often have more control over the *"basic privacy-relevant design decisions"*[364] than controllers or processors have. Of note, eIDAS in its Article 12 does not expressly target data controllers. Hence, all participants of the Interoperability Framework should be considered subjects to the obligation to *"facilitat[e] the implementation of the principle of privacy by design"*.[365]

The duty imposed by Article 25 is qualified. The measures and safeguards shall be *"appropriate"* and *"necessary"*. The legislator provides the criteria that shall be used to judge the appropriateness of the measures: (a) the state of the art; (b) the cost of implementation; (c) the nature, scope, context and purposes of the processing. Selected measures must in any case be effective against (d) the risks for the rights of the data subjects (figure 4.1). The article also provides an example of a data protection goal, that of data minimisation,[366] and an example of a technical measure,[367] pseudonymisation.[368]

[361] GDPR (n 164) art 25(1): *"... the controller shall ..."*

[362] ibid art 28(1).

[363] Of the same opinion Bygrave, *"Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements"* (n 359) 116.

[364] Bygrave, *"Hardwiring Privacy"* (n 345) 16.

[365] eIDAS (n 129) art 12(3)(c).

[366] GDPR (n 164) art 5(1)(c).

[367] ibid rec 78 elaborates on the measures further in a non-exhaustive list: *"Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features."*

[368] An addition that during the Trilogue negotiations only existed in the European Council's draft: EU Parliament: Committee on Employment and Social Affairs, *"Draft Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* (C7-0025/2012 – 2012/0011(COD), 8 November) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

$$\left(\begin{array}{c} state\ of\ the\ art \\ + \\ cost\ of\ implementation \\ + \\ nature,\ scope,\ context,\ purposes\ of\ processing \end{array}\right) > \begin{array}{c} risks\ for\ the\ rights \\ of\ data\ subjects \end{array}$$

FIGURE 4.1: Assessing appropriate measures under GDPR Art 25

As the ambition seems to be to ultimately expand the scope of the use of eID means, in particular in the context of relationships with private-sector services,[369] it is crucial to get the prescription of the principle of data protection by design for eID correctly. More generally, it is essential to properly derive the prescription of data protection by design correctly because operation of eID has effects for trust services, namely in the context of certificate creation and distribution. National eID schemes exist where eID is performed through the use of electronic certificates. The nature and number of attributes contained in certificates are certainly dependent upon national implementations.[370] Simply put, there are cases where data protection by design for eID will produce effects for other trust services as well, as for example in the quantity and quality of the attributes that should be permissible inside an electronic certificate.

The significance of getting data protection by design right is all the more clear since Article 83(4) of the GDPR mandates that infringement of Article 25 is *"subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher."*

In order to assess whether data controllers meet their data protection by design obligations the criteria of Article 25 should be examined in context. In the context of eID as regulated by eIDAS, data controllers include Government Service Providers, Government Identity

[369] eIDAS (n 129) rec 17: *"Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions."*; see also European Commission, *"Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe"* (Communication) COM(2016) 288 final, 11 *"the Commission will further promote interoperability actions, including through issuing principles and guidance on eID interoperability at the latest by 2017. The aim will be to encourage online platforms to recognise other eID means – in particular those notified under the eIDAS Regulation (EC) 910/2014 – that offer the same reassurance as their own."*

[370] For example, certificates used for eID and authentication within the Belgian eID scheme contain a serial number which is identical to a citizen's *"national registration number"* derived from the National Register: Pieter Verhaeghe and others, *"Security and Privacy Improvements for the Belgian eID Technology"* in Dimitris Gritzalis and Javier Lopez, *Emerging Challenges for Security, Privacy and Trust: 24th IFIP TC 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18–20, 2009. Proceedings* (Dimitris Gritzalis and Javier Lopez eds, Springer Berlin Heidelberg 2009) DOI: 10.1007/978-3-642-01244-0_21 238–239. This number includes the date of birth and the gender: *"The National Registry number consists of 11 digits. The first 6 digits stand for the date of birth (2 digits for the year, 2 digits for the month and 2 digits for the day), the 3 following digits stand for the serial number of the registration (even numbers are reserved for women) and the last 2 digits form the verification number (art. 1 et seq Royal Decree 3 April 1984)."* Bert-Jaap Koops and Ronald Leenes, *"Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law"* (2014) 28(2) International Review of Law, Computers & Technology 159 DOI: 10.1080/13600869.2013.801589, 51.

Providers and private-sector Service and Identity Providers inasmuch as the latter are participating in a scheme recognised by the Member State. However, the GDPR falls short of providing a comprehensive methodology to assess data protection by design, relying on data controllers and data processors to decide on a methodology to apply. Besides, any methodology used should be tailored to address the specific complexities of eIDAS and, particularly, the effects of eIDAS Article 12 (the Interoperability Framework).

4.4 Conclusion

The state of the art in system engineering has recognised that soft measures in the form of policies are not enough to accomplish effective protection. Instead, the holistic approach of privacy by design combines policy and technological measures that shall work in parallel. The GDPR extended privacy by design into data protection by design to encompass the obligations of data controllers and processors and to add protection to the rights of the data subjects.

Data protection by design is introduced as a qualified obligation. As a result, the measures necessary to effect data protection by design will depend upon the particularities of the processing and need to be assessed against the risks processing might pose to the rights and freedoms of the data subjects.

Although getting the prescription of data protection by design can result in serious penalties for the data controllers and processors, Article 25 is silent as to the methodology to assess the adequacy of selected measures. To address this shortcoming, the next chapter explains why it is crucial to read GDPR Article 25 in the light of Article 35. Article 35 on data protection impact assessments could provide for a process through which the necessity and feasibility of the engineering of data protection principles and security measures can be assessed. Consequently, after an overview of DPIA methodologies, this thesis proposes a DPIA-based methodology to assess data protection by design with references to its implementation in the field of eID.

Chapter 5

The scope of GDPR Article 35

Taking into account [...] the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
— GDPR Art 25(1)

...the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken...
— GDPR Rec 84

5.1 Introduction

Data protection by design under GDPR Article 25 demands the qualification of several factors for the selection of adequate measures. The GDPR stays silent as to the methodology that data controllers and processors ought to follow to perform this qualification.

However, Article 25 conditions the appropriateness of measures to *"the risks of varying likelihood and severity"*[371] to the data subjects. Likelihood and severity of risks are direct indicators of the obligation of the data controller to perform impact assessments of their processing operations. Article 25, therefore, should be read in light of the obligations for DPIAs of Article 35.

Although, much like data protection by design, Article 35 does not explicitly specify a methodology to be followed, DPIAs have been the focus of several methodological frameworks. This chapter briefly discusses the origins and scope of Article 35 and performs a review of three methodologies for DPIAs. DPIAs are mandatory when the processing is likely to result in high-risks for the data subjects. The general criteria

[371] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 25(1).

to determine when processing is likely to result in high-risks have been discussed in WP29 guidance, which, although not directly legally binding, indicate how national DPAs are expected to apply the GDPR. DPAs are expected to produce national lists of *"processing operations which are subject to the requirement for a data protection impact assessment"*.[372] However, they are free to use criteria that go further than WP29's guidelines, and in practice differences in the interpretation of high-risk processing have been noted.[373] DPAs are also free to publish lists of processing activities that do not trigger the obligation to perform a DPIA.[374] In addition, it is acknowledged that the GDPR provides *"enough scope for different forms of implementation"*,[375] with WP29 actively encouraging the development of diverse DPIA methodologies.[376]

As a result, a number of DPIA methodologies are publicly available. Three criteria were set to select methodologies for review in this chapter: (a) the methodology needed to have a version available in English; (b) its scope should not be sector-specific (unless the sector was eID); (c) it should be developed by an authoritarian source, such as a DPA. Point (c) was considered important because DPAs are the authorities supervising compliance with the obligation of data protection by design. Based on these criteria, three methodologies were selected for review. The UK ICO's, the French CNIL's and the German Independent DPAs.

The three methodologies approach the assessment of risk in a different way. However, all agree that a balancing test in the form of a preliminary risk threshold analysis is necessary in order to determine whether processing is likely to result in high-risks. Reviewing the three methodologies, it is demonstrated that in many cases eID could be considered as a 'high-risk' processing operation that triggers a mandatory DPIA.

Regardless, the chapter argues that a threshold analysis, i.e. a 'light' assessment or 'mini-DPIA', satisfies the criteria of Article 25(1) and can, therefore, be used as a methodology to assess the the appropriateness of data protection by design measures. A suitable framework for a 'light' DPIA will be discussed later in chapter 6.

Section 5.2 presents a short history of DPIAs, with section 5.3 explaining the conceptualisation of DPIAs by Article 35 of the GDPR. Three methodological approaches are introduced next: the ICO's DPIA in section 5.3.1, CNIL's PIA methodology in

[372] GDPR (n 371) art 35(4).

[373] See for example Centre for Information Policy Leadership, *Centre for Information Policy Leadership Comments on Data Protection Authorities' Draft List of Types of Data Processing Operations which Require or Do Not Require a Data Protection Impact Assessment* (2018) ⟨https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_national_dpa_lists_of_high_risk_processing.pdf⟩ accessed 8 May 2020 (archived at ⟨https://bit.ly/2SRB1B5⟩) 11–15.

[374] GDPR (n 371) art 35(5); i.e. where a processing operation may *prima facie* satisfy the general criteria that indicate highly risky processing, but because of its particular circumstances it is unlikely to actually possess risks.

[375] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev 01, 2017) 15.

[376] ibid 16.

section 5.3.2 and the German SDM in section 5.3.3. Section 5.4 examines when the obligation to perform a DPIA applies, and section 5.5 lists the procedural steps needed in order to conduct a DPIA. Finally, section 5.6 discusses the conditions where data processing for eID might be considered as triggering a mandatory DPIA. The material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness.*[377] Part of the material was published under *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"*; *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[378]

5.2 Data Protection Impact Assessments

Risks assessments have been a part of data protection compliance under the name Privacy Impact Assessment (PIA) for decades. The first PIAs emerged in common law jurisdictions around the 1990s,[379] with the UK developing the earliest PIA guidance in the EU in 2007,[380] with a second revision following in 2009.[381] Although Dir 95/46/EC did not explicitly provide for a PIA, Article 20(1) DPD required Member States to *"determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and [...] check that these processing operations are examined prior to the start thereof."* This requirement was implemented in several national law

[377] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[378] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (2017) 3(3) The Journal of Web Science 32 DOI: 10.1561/106.00000010; Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

[379] Roger Clarke, *"Privacy impact assessment: Its origins and development"* (2009) 25(2) Computer Law & Security Review 123 DOI: https://doi.org/10.1016/j.clsr.2009.02.002, 127–129.

[380] Adam P Warren and others, *"Privacy Impact Assessments: the UK experience"* (31st International Conference of Data Protection and Privacy Commissioners, 4–6 November 2009, Madrid) 3–5. For a review of UK contributions to the EU data protection framework, among which the concepts of impact assessments and certification, see Paul de Hert and Vagelis Papakonstantinou, *"The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit"* (2017) 33(3) Computer Law & Security Review 354 DOI: 10.1016/j.clsr.2017.03.008, 357-358.

[381] ICO, *Privacy Impact Assessment (PIA)* (2009) ⟨http://webarchive.nationalarchives.gov.uk/20091204132953/http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx⟩ accessed 20 September 2017.

transpositions of Dir 95/46/EC[382] Besides, prior to the GDPR the Commission had issued two sector-specific (voluntary) PIA policies; a recommendation on radio-frequency identification (RFID) applications,[383] endorsed in its revised form by WP29,[384] and a recommendation for 'Smart Grid' and 'Smart Metering' applications.[385]

5.3 GDPR Article 35

DPIAs are governed by GDPR Article 35. Numerous definitions exist for DPIAs, often referring to them as tools, instruments or processes;[386] Article 29 Working Party views DPIAs as *"a process for building and demonstrating compliance"* with the GDPR.[387]

Under Article 35(1) of the GDPR, controllers shall *"carry out an assessment of the impact of the envisaged processing operations on the protection of personal data"* (i.e. a DPIA). The GDPR does not exhaustively define the content of a DPIA, but provides for a minimum content:[388]

> (a) *a systematic **description of the envisaged processing** operations and the **purposes of the processing**, including, where applicable, the legitimate interest pursued by the controller;*
>
> (b) *an assessment of the **necessity and proportionality** of the processing operations in relation to the purposes;*

[382] Such the transposition in France, Austria, Denmark, Finland, Germany, Greece, Italy, Luxembourg, the Netherlands, Belgium, Portugal and Sweden. The law in Spain did not define which processing operations require prior checks, but gave the data protection authority the liberty to subject processing operations to checks according to will. Note that, even though the law in the UK provided for prior checks, in practice its use has been limited (see Douwe Korff, *Comparative Summary of National Laws: EC Study on Implementation of Data Protection Directive* (, Human Rights Centre, University of Essex 2002) 173–175) and has been seen as a basis for the development of PIAs methodologies, albeit in the form of soft law, guidance and proposals (David Wright and others, *A Privacy Impact Assessment Framework for data protection and privacy rights: PIAF Project* (Deliverable D1, 2011) 198–199.

[383] European Commission, *"Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200)"* (Commission Recommendation) C(2009) 3200.

[384] Article 29 Data Protection Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (WP 180, 2011).

[385] European Commission, *"On the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems"* (Commission Recommendation) 2014/724/EU..

[386] Felix Bieker and others, *"A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation"* in Stefan Schiffner and others, *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016) DOI: 10.1007/978-3-319-44760-5_2 21–22.

[387] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 4.

[388] For an account of the variations of the minimum content during the 'Trilogue' negotiations, see David Barnard-Wills and Vagelis Papakonstantinou, *Best Practices for cooperation between EU DPAs* (Phaedra II project Deliverable 2.2, version 1.0, 2016) ⟨http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II_D2.2-report_2016.02.15.pdf⟩ accessed 15 March 2020 (archived at ⟨https://bit.ly/2LYtlZY⟩) 56.

(c) *an assessment of the* ***risks to the rights and freedoms of data subjects*** *referred to in paragraph 1; and*

(d) *the* ***measures*** *envisaged to* ***address the risks****, including safeguards, security measures and mechanisms to ensure the protection of personal data and to* ***demonstrate compliance*** *with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.* [emphasis given][389]

WP29 has issued guidelines in order to clarify what type of analysis is expected in a DPIA;[390] at the same time national Data Protection Authorities (DPAs) have also put together guidelines and templates for DPIAs[391] and relevant work is ongoing at the level of international standards' specification.[392] These guidelines and templates remain high-level enough to be applicable to all sectors.

5.3.1 The UK Information Commissioner's Office (ICO) Privacy Impact Assessment Methodology

Prior to the GDPR the ICO had issued a code of practice for DPIAs on 25 February 2014. In it, a DPIA is defined as *"a process which assists organisations in identifying and minimising the privacy risks"*.[393] The DPIA is meant to support any given project that processes personal data throughout its entire lifecycle. The DPIA process is divided into seven steps, in order to: (a) identify the need for a DPIA; (b) describe the information flows; (c) identify the privacy and related risks in relation to both data subjects rights and risks for the organisation; (d) identify and evaluate the privacy solutions in a tiered approach – from elimination to acceptance; (e) sign off and record the outcomes; (f) integrate the outcomes into the project's plan; and (g) consult with internal and external stakeholders as needed throughout the process.[394] The Code of practice did not list specific risks and measures. It instead used generic advice for risk management that was meant to be flexible enough to be adapted to the needs of any project.

[389] GDPR (n 371) art 35(7).

[390] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375).

[391] e.g. CNIL, *Privacy Impact Assessment (PIA): Measures for the Privacy Risk Treatment* (2015); CNIL, *Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)* (2015) ⟨https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf⟩ accessed 15 August 2018 (archived at ⟨https://tinyurl.com/y9cqnmw4⟩); CNIL, *Privacy Impact Assessment (PIA): Tools (templates and knowldge bases)* (2015) ⟨https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf⟩ accessed 15 August 2018; Conference of the Independent Data Protection Authorities of the Bund and the Länder, *The Standard Data Protection Model* (v1.0, 2017); *Privacy Impact Assessment (PIA)* (n 381); White Wire Data Protection, *Data Protection Impact Assessment* (Template, 2017) ⟨https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6590736/bin/18-1421-Techapp-s3.pdf⟩ accessed 26 May 2018 (archived at ⟨https://tinyurl.com/ybc5fz9q⟩).

[392] In particular with ISO 31000:2009; ISO/IEC 29134; and the ongoing ISO/IEC 27005:2011.

[393] ICO, *Conducting Privacy Impact Assessments: Code of Practice* (v 1.0, 2014) 5.

[394] ibid 11.

The Code of Practice of 2014 was replaced by a new set of guidelines on 22 March 2018. The new guidelines define a DPIA as a way to *"systematically and comprehensively analyse [data] processing and help [...] identify and minimise data protection risks."*[395] The process has now been broken down into nine steps: (a) identify a need for a DPIA; (b) describe the processing; (c) consider consultation; (d) assess necessity and proportionality; (e) identify and assess risks; (f) identify measures to mitigate risks; (g) sign off and record outcomes; (h) integrate outcomes into plan; and (i) keep under review.[396] Arguably, of significant importance is the final step, the continuous review, that signifies that – in line with data protection by design – the DPIA plays a role throughout the lifetime of a project. Contrary to the previous code of practice, the new guidance includes a list of *"non-exhaustive examples"* of processing operations that require a mandatory DPIA,[397] and exemplary lists of possible risks and measures.[398]

5.3.2 The French Commission Nationale De L'Informatique Et Des Libertès (CNIL) PIA

The CNIL also views DPIA as a continuous cycle, starting with the definition of data flows, the purposes for processing, the persons concerned, the proportionality and necessity of the operation and the planned control mechanisms.[399] The CNIL offers a scale to measure the impact of processing operations.[400] It also complements the methodology with a step-by-step template for DPIAs and a set of suggested risk-treatment controls.[401]

The CNIL updated their guidance in February 2018 to bring it in line with the GDPR.[402] However, their DPIA methodology does not specify when the need to carry out a DPIA arises.[403] The CNIL points out how DPIAs not only demonstrate accountability of the data controller, through the compliance checks and applied controls, but also data protection by design.[404] The methodology explains how an assessment of the risks should be carried out,[405] and the separate knowledgebase provided includes typologies of feared

[395] ICO, *Data Protection Impact Assessments (DPIAs): The General Data Protection Regulation: Accountability and Governance* (v1.0.123, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf⟩ accessed 14 May 2019 (archived at ⟨http://archive.fo/dCyj4⟩) 4.

[396] ibid 6.

[397] ibid 39–41.

[398] ibid 31–35.

[399] CNIL, *Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)* (n 391) 7–9.

[400] CNIL, *Privacy Impact Assessment (PIA): Tools (templates and knowldge bases)* (n 391).

[401] ibid 8–9.

[402] CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf⟩ accessed 25 May 2019; CNIL, *Privacy Impact Assessment (PIA): Methodology* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf⟩ accessed 25 May 2019; CNIL, *Privacy Impact Assessment (PIA): Templates* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf⟩ accessed 25 May 2019.

[403] CNIL, *Privacy Impact Assessment (PIA): Methodology* (n 402) 2: *"The methodology does not address the initial conditions which determine whether or not a PIA needs carrying out"*.

[404] CNIL refers to *"privacy by design"* but points to GDPR (n 371) art 25: CNIL, *Privacy Impact Assessment (PIA): Methodology* (n 402) 2.

[405] ibid 6–7.

events (risks) and possible outcomes,[406] as well as details on possible measures,[407] without though making clear which risks each measure is supposed to address.[408] The measures are divided into (physical and logical) security and organisational controls.[409]

5.3.3 The German Standard Data Protection Model (SDM)

The Standard Data Protection Model (SDM) was developed by the independent DPAs of Germany. It has a clear focus on legal compliance with the German Data Protection laws and it has been updated to address the legal requirements of the GDPR. The SDM aims to help data protection authorities and the public to trace a project's compliance through a predefined list of evaluation criteria. The SDM translates legal requirements into data protection goals.[410] Although strictly speaking the SDM does not attempt to formulate a full DPIA methodology, it offers resources to reach compliance with the GDPR.[411] To assess whether the data protection goals are met a list of controls is offered. A catalogue of more specific data measures organised per level of protection is currently being developed by the German DPAs, and will be annexed to the SDM.[412] In order to evaluate the significance of the risks, the SDM proposes what it names the *"level of interference"*:[413] a measure based on the corresponding legal basis, the level of protection (i.e. the safeguards in place), the duration of storage and the type and number of potential recipients of the data,[414] which is meant *"to evaluate the significance of the risks to the right to informational self-determination"*,[415] i.e. the rights and freedoms of individuals. The level of interference, in other words, is quite similar to the criteria to assess the severity and likelihood of risks set by the CNIL.[416]

[406] ibid 2–3.

[407] ibid 11–103.

[408] ibid 13–17.

[409] ibid 18–19.

[410] *The Standard Data Protection Model* (n 391) 6.

[411] ibid 6: *"The model is, on the one hand, directed at controllers who are enabled through recourse to the SDM, to systematically plan, implement and continuously monitor the necessary functions and protection measures. On the other hand, the model is also aimed at supervisory authorities and enables them to reach a transparent and plausible, reliable judgment on a procedure and its components."*

[412] Ch 7 of the SDM, not included in this version: ibid 3.

[413] ibid 33: *"Any processing of personal data by an organisation constitutes an interference with the right to informational self-determination."* The *"right to informational self-determination"* refers to *"the free development of personality under modern conditions of data processing requires the individual to be protected against the unlimited collection, storage, usage, and transfer of his or her personal data. "*

[414] ibid 33: *"A measure for the level of interference is, inter alia, the purpose of the data processing that is determined by the corresponding legal basis, the level of protection, the duration of storage, the type and the number of possible recipients of the processed data."*

[415] ibid 33.

[416] See nn 399 and 405. Severity and likelihood are dependent on the level of identification of personal data, the nature of risk sources, the number of interconnections and the number of recipients: see n 475.

5.4 The Obligation to Perform a DPIA

The DPIA is mandatory when the processing of personal data is *"likely to result in a high risk to the rights and freedoms of natural persons."*[417] Although the GDPR does not specify all the situations in which a high risk is likely to occur, it does note that special consideration should be given to processing using new technologies. Article 35(3) lists three instances for which a DPIA is required, although this list is not exhaustive. In particular, a high risk should be initially presumed in cases of:

> a) *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
>
> b) *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
>
> c) *a systematic monitoring of a publicly accessible area on a large scale.*[418]

In this sense, DPIAs depart from traditional risk management assessments, which only focus upon the risks to the organisation, i.e. the data controller, and its activities. The primary focus of a DPIA must be the risks posed to the rights and freedoms of data subjects.[419] The GDPR offers examples of such risks in Recital 75, some of which with particular importance for eID and authentication, e.g. risks to identity theft or fraud; unauthorised reversal of pseudonymisation.[420]

An exception to mandatory DPIAs exist if (a) the legal basis for the processing is mandated by EU or national law and, (b) a DPIA has already been carried out in the

[417] GDPR (n 371) art 35(1).

[418] ibid art 35(3).

[419] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 14.

[420] GDPR (n 371) rec 75: *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."*

context of the adoption of this legal basis.[421] In this case, it is up to the Member State to request an optional DPIA prior to the processing.

Failure to conduct a DPIA when needed, or conducting a DPIA in a wrong way can result in administrative fines of up to 10.000.000€ or up to 2% of the annual turnover of the preceding financial year, whichever is higher.[422]

In an attempt to clarify which processing operations could result in *"high risk"*, WP29 posits nine criteria:[423]

(1) Processing for evaluation or scoring, profiling and predicting;
(2) Automated decision making with legal or similar significant effect;
(3) Systematic monitoring;
(4) Sensitive data or data of a highly personal nature;
(5) Data processed on a large scale;
(6) Matching or combining data sets;
(7) Data concerning vulnerable data subjects;
(8) Innovative use of applying new technologies;
(9) Processing that prevents data subject from exercising a right or using a service or a contract.[424]

According to WP29 a DPIA should be mandatory when two or more of these criteria are met.[425] However WP29 notes that in some cases a controller can consider that processing which meets only one of these criteria requires a DPIA.[426] Additionally, some national DPAs advice that carrying out a DPIA, even when it is not mandatory, can help towards practical demonstration of compliance with the GDPR's Article 25 *"Data Protection by Design and by Default"*.[427]

DPAs are tasked with creating lists of processing operations that require mandatory DPIAs.[428] They can also limit the catalogue of processing operations by listing cases where DPIAs are not needed. Controllers are free to select the method of assessment

[421] ibid art 35(10).
[422] ibid art 83(4)(a).
[423] Note that the draft version contained a tenth criterion: when processing involved international transfers.
[424] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 9–11.
[425] ibid 10.
[426] ibid 11.
[427] ICO, *Preparing for the General Data Protection Regulation (GDPR)* (v2.0, 2017) ⟨https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf⟩ accessed 24 September 2019 (archived at ⟨http://archive.fo/8EuSp⟩) 8; ICO, *Guide to the General Data Protection Regulation* (1,0,154, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf⟩ accessed 24 May 2018 (archived at ⟨https://tinyurl.com/y9pr9o2x⟩) 183: *"DPIAs are an integral part of data protection by design and by default."*
[428] GDPR (n 371) art 35(4).

where a need for a DPIA arises. In this respect, controllers have a fair amount of discretion:[429] Apart from defining the DPIA methodology,[430] they determine if their processing operation does not result in a risk sufficient to trigger a mandatory DPIA,[431] choose qualified assessors and ensure their independence,[432] document the process and guarantee its robustness.[433] So far, the DPAs of Belgium (at the time Belgium's Privacy Commission), Poland and the UK have published versions of their lists. The lists are in line with the criteria set by WP29. However, different DPAs expand or narrow those criteria. For example, as regards automated decision making, the Polish authority considers that a mandatory DPIA is triggered when there are any legal, physical, financial or other effects on natural persons.[434] The Belgian authority, though, requires that, in addition, the data used are sourced from a third party without the specific consent of the data subject.[435] Additionally, there are cases where the national authorities introduce

[429] Dariusz Kloza and others, *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals: d.pia.lab Policy Brief* (2017) 3.

[430] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 15: *"The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices"*; ibid 17: *"It is up to the data controller to choose a methodology"*.

[431] ibid 10: *"if the controller believes that [...] it is considered not to be 'likely high risk', he has to thoroughly document the reasons for not carrying out a DPIA."*.

[432] ibid 13: *"Carrying out the DPIA may be done by someone else, inside or outside the organization..."*.

[433] ibid 13: *"...but the controller remains ultimately accountable for that task."*

[434] Polish Data Protection Authority, *Proposed list of processing types for which a data protection impact assessment is mandatory* (2018) ⟨https://iapp.org/media/pdf/resource_center/Mandatory-DPIA-Poland-klattorneys.pdf⟩ accessed 22 June 2019 (archived at ⟨https://bit.ly/2Xpsjf6⟩) 1–4. Full list of criteria: Evaluation or assessment, including profiling and prediction (behavioural analysis) for purposes that may have negative legal, physical, financial or other effects on natural persons; automated decision making that produces legal, financial or similar material results; systematic large-scale monitoring of publicly accessible places using elements of recognition of features or properties; processing of special categories of personal data concerning convictions and law infringements (sensitive data according to WP29); large-scale data processing, with large scale defined according to the number of people whose data are processed, the scope of processing, the retention periods and the geographical scope; performing comparisons, assessment of or drawing conclusions based on the analysis; processing data concerning persons whose assessment and the services they are provided with depend on entities or persons which have authoritative and/or assessment-related powers; innovative use or application of technological or organizational solutions; cross-border data transmission outside the European Union; processing that *"prevents data subjects from exercising their rights or using a service or a contract"*.

[435] Belgian Commission for the Protection of Privacy, *Recommandation relative au Registre des activités de traitements (article 30 du RGPD)* (Recommandation nº 06/2017 (CO-AR-2017-011), 2017) ⟨https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/04/Belgian-Privacy-Commission-Recommendation_French.pdf⟩ accessed 25 April 2019 (archived at ⟨http://archive.fo/6a9nn⟩) Annex 3. Full list of criteria: where biometric data are used to identify people in public or publicly accessed spaces; where data from a third party are used for automated decision making; where special categories of data are used for purposes other than that for which they were originally collected, unless specific consent has been given or in order for the controller to meet its legal obligations; where processing is carried out using a medical implant and the breach could jeopardise the data subject's health; where data concerning vulnerable population are processed for a purpose other than that they originally were collected for on a large scale; where data from third parties are processed on a large scale to predict the economic situation, health, personal preferences or interests, reliability or behaviour, or location or movements of individuals; where special categories of data are systematically shared between controllers; where data from Internet of Things devices are processed on a large scale to predict the economic situation, health, personal preferences or interests, reliability or behaviour, or location or movements of individuals; where special categories of data are systematically shared between controllers; where processing of data on a large scale and/or systematic processing from telephony data, internet data, or other communication

new categories of processing as *"high-risk"*. In the Polish list, two such categories are introduced: processing for marketing reasons when combining data from different sources and processing for candidate matching or whistleblowing systems.[436]

The UK ICO lists processing operations that require a DPIA. Many of these operations mirror the types selected by WP29:

(1) New technologies (or the novel application of existing technologies);
(2) Denial of service (including automatic decision making and profiling or processing of special categories of data);
(3) Large-scale profiling (but without a precise definition of what constitutes *"large-scale"*);[437]
(4) Biometrics;
(5) Genetic data (other than from a health professional for the health care of the data subject);
(6) Data matching (combining, comparing or matching personal data from multiple sources);
(7) Invisible processing (when processing personal data that have not been obtained directly by the data subject as per GDPR Article 14);
(8) Tracking (of geolocation or behaviour, whether online or offline);
(9) Targeting of children or vulnerable individuals (for marketing purposes, profiling or automated decision-making);
(10) Risk of physical harm (in cases where a personal data breach would jeopardise the physical health or safety of individuals).[438]

Of significance is the list of high-risk processing examples that is included at the end of the guidance:[439] The ICO expressly includes *"Federated identity assurance services"* as an example of data matching processing that is likely to result in high-risk[440] and, therefore, processing that requires a DPIA.[441] Identity management services are explicitly

data, metadata, location data of natural persons, or data which permits the organisation to find natural persons and the processing is not necessary in order to provide a service to the data subject; where data are processed on a large scale and the behaviour of individuals is observed, collected, established or influenced, including for advertising purposes, in a systematic manner using automated processing.

[436] Note also that the Belgian Privacy Commission has been replaced by a new body, the Belgian DPA, on 25 May 2018.

[437] Instead, examples are given in *Data Protection Impact Assessments (DPIAs)* (n 395) 23: A hospital processing patient data; tracking individuals using a city's public transport system; a fast food chain tracking real-time location of its customers; an insurance company or bank processing customer data; a search engine processing data for behavioural advertising; or a telephone or internet Service Provider processing user data. Further examples are included in pp 39–41.

[438] ibid 20.

[439] ibid 42–44.

[440] ibid 19: *"This does not mean that these types of processing are always high risk, or are always likely to cause harm – just that there is a reasonable chance they may be high risk and so a DPIA is required to assess the level of risk in more detail."*

[441] ibid 42.

mentioned also in the list of the Estonian DPA.[442] The Spanish DPA, AEPD, does not explicitly mention identity authentication. However, the list of processing operations likely to result in high-risks includes *"processing of unique identifiers that allow the identification of users of services of the information society"*.[443] An analogous approach has been adopted by the Greek DPA, HDPA, for operations *"concerning the national identity number or other identifiers of general application"*.[444]

5.5 The Procedural Steps for a DPIA

A complete DPIA should be conducted in three stages: A preparatory phase, an evaluation phase and an auditing (or reporting) phase.[445]

In preparation for a DPIA the controller(s) should consider whether there is a legal obligation to carry out a DPIA, in line with what is discussed in section 5.4. Alongside the lists of processing operations that require mandatory DPIAs, and their exceptions, from national DPAs,[446] the controllers should consider whether they are engaging in activities as outlined in Article 35(3) and WP29's interpretation of the concept of *"high risk"* processing.[447] For this purpose, a description of the data processing operations is required (the scope of the processing).[448] Such a description[449] should include considerations relating to the purposes of the processing (according to the corresponding legal bases)[450] and to strategies for ensuring compliance with the data protection principles.[451] Particular attention should be given to the data formats, the protocols for transfer and storage

[442] Data Protection Inspectorate, *List of cross-border processing operations which are subject to the requirement for a data protection impact assessment* (2019) ⟨https://edpb.europa.eu/sites/edpb/files/decisions/ee_estonian_cross-border_dpia_list.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2zYrkdH⟩) no. 7: *"particularly in digital trust services and in comparable identity management services"*.

[443] AEPD, *List of the types of data processing that require a data protection impact assessment under Art. 35.4* (2019) ⟨https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2ZCHtjA⟩) 2.

[444] HDPA, *List of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of GDPR* (2018) ⟨http://www.dpa.gr/pls/portal/url/ITEM/7DBBF465EC436645E050A8C07C2422DA⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/3cYfOO9⟩) s 2.2.3; an identical decision has been taken by the Cypriot DPA: Office of the Commissioner for Personal Data Protection, *Indicative List of Processing Operations Subject to DPIA Requirements under Article 35(4) of the GDPR* (2019) ⟨http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/ED786DE02E8020FCC225826000377143/$file/Indicative%20DPIA%20list.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2WVoor9⟩) no. 1.

[445] Bieker and others (n 386) 26.

[446] GDPR (n 371) arts 35(4), 35(5).

[447] See section 5.4.

[448] CNIL, *Privacy Impact Assessment (PIA): Methodology* (n 402); *The Standard Data Protection Model* (n 391); *Conducting Privacy Impact Assessments: Code of Practice* (n 393); *Data Protection Impact Assessment* (n 391).

[449] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 9.

[450] GDPR (n 371) art 6.

[451] ibid art 5.

and the technology used.[452] All stakeholders should be identified at this stage, including the data subjects.[453] The role of the preparation stage is to assess whether processing is *"likely to result in high risk"* and, therefore, triggers the mandatory DPIA of Article 35. The preparation, in other words, is a threshold analysis,[454] whose purpose is to screen *"for any red flags which indicate that you need to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail."*[455] This concept of a threshold analysis is further expanded infra[456] as a tool to assess the adequacy of data protection by design measures.

After the preparatory stage, an evaluation stage should follow. In the evaluation stage, the processing operations are assessed for potential risks against the GDPR's objectives for the rights and freedoms of data subjects.[457] The German SDM calls these objectives *"data protection goals"*,[458] and divides them into seven categories: Data minimisation, Availability, Integrity, Confidentiality, Unlinkability, Transparency and Intervenability (see section 6.2).

The evaluation stage requires the measuring of the risks the processing operations are posing to the rights and freedoms of individuals against the data protection goals. Several scales have been proposed to measure these risks. The German SDM proposes a scale based on the concept of *"level of interference"*.[459] The scale builds on the methodology of the Federal Office for Information Security (BSI) for IT security,[460] but is adapted for data protection. As a starting point, the SDM considers that all data processing operations always impact on (or interfere with) the rights and freedoms of individuals (the *"level of interference"*). Accordingly, based on the level of interference a *"level of protection"* is required. All processing operations involving personal data are then assumed to require at least a *"normal"* level of protection.[461] The level *"normal"* seems to represent a baseline level of protection. Further, the SDM provides that when certain categories of data are processed, a *"high"* level of protection is necessary. Such categories

[452] *The Standard Data Protection Model* (n 391) 31–32.

[453] *Data Protection Impact Assessment* (n 391) 5; *The Standard Data Protection Model* (n 391) 31; CNIL, *Privacy Impact Assessment (PIA): Methodology* (n 402) 11; *Conducting Privacy Impact Assessments: Code of Practice* (n 393) 33.

[454] Or, in the ICO's terms a *"high-level screening test"*: *Data Protection Impact Assessments (DPIAs)* (n 395) 19.

[455] ibid 19.

[456] See chapter 6.

[457] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 17: *"the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective"*.

[458] *The Standard Data Protection Model* (n 391) 22–23.

[459] ibid 33.

[460] Federal Office for Information Security [BSI], *IT-Grundschutz Methodology: BSI-Standard 100-2* (v 2.0, 2008) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile⟩ accessed 25 April 2019 (archived at ⟨http://archive.fo/nzytR⟩).

[461] Since processing of personal data is always an interference, a lower level can only be achieved if no personal data are processed: *The Standard Data Protection Model* (n 391) 34.

are considered to be, for example, the processing of non-modifiable personal data (like biometric and genetic data); the processing of highly linkable data (like a health insurance number of a tax ID); processing of data with a lack of transparency for the data subjects (the lack of transparency has to be justified legally); processing in procedures with potentially serious consequences for the data subject's finance, reputation or physical integrity; processing which can have impact on the exercise of fundamental rights of a large number of data subjects; processing that results in a risk of discrimination or stigmatisation; and processing that results in intervention in particularly protected areas of life of a data subject.[462] Finally, in such processing operations where the data subject is *"directly and with vital significance dependent on the decisions or services"*, or *"where the effects of a processing cannot come to the attention of the data subject"*,[463] a *"very high"* level of protection is required. However, the SDM in its current version does not provide a definition of the impact that the level of interference has on the data subjects. For reference, BSI's methodology on IT security defines the impact of operations corresponding to a *"normal"* level as *"any loss or damage [that] is limited and calculable"*, a *"high"* level as *"any loss or damage [that] may be considerable"* and a *"very high"* level as *"any loss or damage [that] may be of catastrophic proportions which could threaten the very survival of the organisation."*[464]

Additionally, pending the full catalogue of measures the SDM will propose, there is no classification of measures that satisfy a *"normal"*, *"high"* or *"very high"* level of protection. Going back to BSI's IT security methodology, it seems that the distinction should be based on the fact that although the standard safeguards should be present for each of the three levels, in a *"high"* level scenario the standard safeguards *"may not be sufficient alone under some circumstances. Additional safeguards can be determined by performing a supplementary security analysis"*,[465] whereas in a *"very high"* scenario the standard safeguards *"are generally not sufficient on their own. The required additional safeguards must be determined individually on the basis of a supplementary security analysis."*[466] Bieker and others, explaining the methodology, illustrate the difference through an example of a confidentiality safeguard:[467] A scheme, in order to satisfy the confidentiality goal, might implement a *"rights and roles concept"* (access control). However, the mere implementation of access control is not enough. The roles assigned and the rights granted to each role have to be analogous to the level of protection warranted by the particular type of processing.

The CNIL's PIA methodology, on the other hand, proposes a two-axis scale for identifying levels of protection (what it calls *"estimating severity"*).[468] One axis measures the impact

[462] *The Standard Data Protection Model* (n 391) 34.
[463] ibid 35.
[464] Federal Office for Information Security [BSI], *IT-Grundschutz Methodology* (n 460) 48.
[465] ibid 59.
[466] ibid 59.
[467] Bieker and others (n 386) 32–33.
[468] CNIL, *Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)* (n 391) 6.

a risk will have on individual's rights and freedoms, using four levels:[469] *"Negligible"*, when data subjects are not expected to be affected or are expected to overcome the inconveniences caused without any problem; *"limited"*, when data subjects may encounter significant inconveniences which they nevertheless overcome; *"significant"*, when data subjects face significant consequences, which they should be able to overcome; and *"maximum"* when data subjects face significant or irreversible consequences which they may not overcome. The other axis of the matrix uses the same categories to estimate the likelihood of a risk materialising: *"Negligible"*, when it does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets; *"Limited"* when it seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets; *"Significant"* when it seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets; and *"Maximum"*, when it seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets. In the 2018 update of the guidelines, the two metrics are presented as separated,[470] and it is then proposed that the two be added together to determine the level of risk.[471] It is not explained how the two metrics should be added together, but it should be assumed that the end result will be similar to the matrix proposed in the previous guidance.[472]

Regardless of the measure used, the level of impact is raised when additional factors are present. In the SDM, attention is drawn to cases in which the level of protection escalates because of their scale or scope: data with a normal level of protection may require a higher level when processed in large quantities[473] or if processed by various controllers with different roles and rights.[474] The CNIL warns that the level of the impact might be raised depending on additional factors such as the level of identification of personal data, the nature of risk sources, the number of interconnections or the number of recipients,[475] as might the likelihood.[476]

After the evaluation stage, safeguarding measures for each of the data protection goals should be considered. The CNIL suggests identifying three types of measures called

[469] In the 2018 update of the guidance, these are contained in CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 402) 4–5.

[470] ibid 4–6.

[471] ibid 6.

[472] CNIL, *Privacy Impact Assessment (PIA): Tools (templates and knowldge bases)* (n 391) 22.

[473] *"Accumulation of a great number of data"*: *The Standard Data Protection Model* (n 391) 36.

[474] *"Accumulation of a great number of rights"*: ibid 36.

[475] CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 402) 5: *"level of identification of personal data; nature of risk sources; number of interconnections (especially with foreign sites); number of recipients (which facilitates the correlation between originally separated personal data)."*

[476] ibid 6: *"opening on the Internet or a closed system; data exchanges with foreign countries or not; interconnections with other systems or no interconnection; heterogeneity or homogeneity of the system; variability or stability of the system; the organization's image."*

"selected controls": (a) organisational controls,[477] (b) physical security controls,[478] and, (c) logical security controls.[479] In the updated guidance, these controls have been replaced with *"controls bearing specifically on the data being processed"*, *"general security controls regarding the system in which the processing is carried out"* and *"organizational controls"*.[480]

In the guidance of 2014,[481] the ICO encourages the adoption of *"appropriate privacy solutions"* and provides general categories of measures.[482] In the updated version of the guidance, the ICO simply includes a general list of measures, noting that the list is purely illustrative.[483] The controllers should assess the safeguarding measures against the identified data protection risks, with three possible outcomes: either the data protection risk is eliminated, reduced or accepted.[484] The controller should document the reasons for which the measure and the resulting outcome are endorsed and justify how the upshot[485] complies with data protection principles.

The German SDM contains more specific guidance. For every protection goal the SDM lists generic measures,[486] while a full catalogue of data protection measures per data protection goal is still pending.[487] In any case, controllers are encouraged to adopt the measures best suited for their specific processing operations. All controls should

[477] CNIL, *Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)* (n 391) 13: *"organization, policy, risk management, project management, etc."*

[478] ibid 13: *"physical access control, security of hardware, protection against non-human risk sources, etc."*

[479] ibid 13: *"anonymization, encryption, backups, data partitioning, logical access control, etc."*

[480] CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 402) 7. Note however that the controls offered in ibid are not classified according to the category they belong.

[481] *Conducting Privacy Impact Assessments: Code of Practice* (n 393).

[482] ibid 28: *"Deciding not to collect or store particular types of information; Devising retention periods which only keep information for as long as necessary and planning secure destruction of information; Implementing appropriate technological security measures; Ensuring that staff are properly trained and are aware of potential privacy risks; Developing ways to safely anonymise the information when it is possible to do so; Producing guidance for staff on how to use new systems and how to share data if appropriate; Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests; Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary; Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf; Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with."*

[483] *Data Protection Impact Assessments (DPIAs)* (n 395) 33: *"deciding not to collect certain types of data; reducing the scope of the processing; reducing retention periods; taking additional technological security measures; training staff to ensure risks are anticipated and managed; anonymising or pseudonymising data where possible; writing internal guidance or processes to avoid risks; using a different technology; putting clear data sharing agreements into place; making changes to privacy notices; offering individuals the chance to opt out where appropriate; or implementing new systems to help individuals to exercise their rights."*

[484] *Conducting Privacy Impact Assessments: Code of Practice* (n 393) 28; *Data Protection Impact Assessments (DPIAs)* (n 395) 34.

[485] *Conducting Privacy Impact Assessments: Code of Practice* (n 393) 29; *Data Protection Impact Assessments (DPIAs)* (n 395) 34. In the updated version the controller also consults their Data Protection Officer.

[486] *The Standard Data Protection Model* (n 391) 27–30.

[487] Thomas Probst, *"Generische Schutzmaßnahmen für Datenschutz-Schutzziele"* (2012) 36 Datenschutz und Datensicherheit - DuD 439 , 442–443.

be determined in line with the state of the art, as mandated by Article 25(1) of the GDPR.[488] There is no requirement to go beyond the state of the art.

5.6 eID as High Risk Processing

eID and authentication schemes are not expressly listed within the 3 instances for which a DPIA is required as per Article 35(1). The eID schemes targeted by eIDAS do not use eID data to profile users, in the sense of the GDPR,[489] or process special categories of data as defined by GDPR Articles 9(1) and 10,[490] and do not monitor publicly accessible areas. Furthermore, in cases of governmentally operated eID schemes, the processing operations are usually mandated by national law;[491] which means that if a DPIA has been carried out during the adoption of the law, there is no obligation to conduct another DPIA prior to the processing.[492]

The foregoing holds true however, as long as the focus is only upon the data contained within the eID means. Assuming all processing activities enabled by eID and authentication are considered, then profiling or the processing of sensitive data could take place, i.e. when a health service provider uses eID to grant access to a patient's medical records.

In any case, the processes of eID and authentication under eIDAS seem to satisfy the criterion of *"data processed on a large scale".* WP29 refers back to its WP243 guidelines[493] to assess what constitutes large scale: The number of data subjects concerned has to be a significant proportion of the relevant population; the data items being processed have to be of a high volume or a wide range; the duration or permanence of the processing activity has to be significant; and the processing operation has to have a geographical extent. It is safe to assume that in the case of eID and authentication for public services at least three of the four factors are being met, at least in cases where the take up of the

[488] In conjuction with GDPR (n 371) arts 32 and recs 78 and 83.

[489] ibid rec 71: *"in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her."*

[490] ibid rec 75: *"where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;"*.

[491] See eg Austria Federal Act on Provisions Facilitating Electronic Communications with Public Bodies 2004, BGBl I Nr. 10/2004, amended by BGBl I Nr. 7/2008 and BGBl I Nr. 59/2008 [Austrian Federal Law] (Austrian E-Government Act 2004) s 1; Germany Gesetz zur Förderung des elektronischen Identitätsnachweises (PAuswG-E) 2017, BGBl. I P. 2745 (Law for the Promotion of Electronic Identification) para 1. *Cf* the UK's Gov.UK Verify based on a public-private partnership, where the processing operations are governed by public services' contracts between the UK Government and private sector suppliers: Cabinet Office, *Framework Agreement and Schedules* (Draft v0,9, 2014) ⟨http://data.gov.uk/data/contracts-finder-archive/contract/1690273/⟩ accessed 24 August 2019 4.

[492] GDPR (n 371) art 35(10).

[493] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375).

national scheme by the population is significant and a large percentage of public services are accessible online. Additionally, cross-border identification and authentication should fulfil the additional criterion of *"matching or combining datasets"*.[494]

Finally, cross-border eID and authentication should be classified as an *"innovative use or appl[ication of] new technological or organisational solutions"* as they extend eID technologies beyond their original jurisdictions and/or targeted services. After all, new technological solutions should not be interpreted to encompass only novel technologies. Instead, the combination of existing technologies into *"novel forms of data collection and usage"*[495] should also be included, as *"[f]or privacy and data protection, the combination of data from various sources can have very significant impacts."*[496] Processing operations that aim at *"allowing, modifying or refusing data subjects' access to a service or entry into a contract"*[497] are also considered as being likely to result in high risk by WP29. The criterion can be applicable in cases where data subjects are denied the exercise of a right or access to a service as the result of *"the processing in itself"*,[498] in other words as a result of a failed identification.[499]

WP29 considers that processing that meets two or more of its criteria should require a DPIA. As demonstrated above, operators of eID schemes that participate in the eIDAS framework shall therefore be expected to conduct a DPIA prior to the processing operations.[500] Regardless, the WP29 highlights that the *"mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects."*[501] Yet, a DPIA will assist controllers in continuously monitoring the risks created by their processing activities.

[494] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 10.

[495] ibid 10.

[496] Barnard-Wills and Papakonstantinou (n 388) 29; see also ibid fn 94 citing European Group on Ethics in Science and New Technologies, *Opinion on Ethics of Security and Surveillance Technologies* (No. 28, 2014) DOI: 10.2796/22379 33: *"While regulation of separate functions e.g. in telecommunications or the use of DNA in identifying an individual has been possible, the real challenge will be in regulating combined functions"*.

[497] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 11.

[498] ibid 11.

[499] This should be distinguished from access control, conversely for cases where the user is indeed successfully identified but has not the right to access a service. Instead, a failed identification in this context refers to such cases where the user, though providing their identity data, cannot be successfully identified and thus the authentication fails.

[500] See also *Data Protection Impact Assessments (DPIAs)* (n 395) 21: *"In most cases, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule. You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high risk, but you should document your reasons. On the other hand, in some cases you may need to do a DPIA if only one factor is present – and it is good practice to do so."*

[501] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (n 375) 6.

Regardless of an obligation to carry out a DPIA, an assessment of the risks of processing will be required in order to determine the appropriate measures to satisfy data protection by design. In the absence of an obligation to perform a DPIA, or where a full DPIA has not yet been performed, this assessment can be performed through the means proposed to assess whether Article 35 is triggered. The threshold analysis required to screen for high-risk (a) details the processing purposes, (b) records the data collected and (c) investigates the existence of potential risks. In other words, the threshold analysis includes the criteria of Article 25(1). Performing a threshold analysis, therefore, can contextualise the processing against the criteria of Article 25 and assess the appropriateness of the technical and organisational measures.[502] Yet, as with conducting a DPIA, there is no consensus as to the methodology to perform this threshold analysis. A suitable framework for data protection by design is proposed in chapter 6.

5.7 Conclusion

The process of a DPIA under Article 35 provides a way to assess the severity and likelihood of the risks of processing to the rights and freedoms of the data subjects. During the DPIA process the processing operation in question is examined against the bulk of the obligations set forth by the GDPR. As a result, a DPIA methodology effectively already incorporates the criteria set in Article 25 and can assist when assessing the appropriateness of the measures for data protection by design.

The three DPIA methodologies examined present variations of a DPIA process. The CNIL DPIA focuses mainly on the satisfaction of the data protection principles of Article 5. However, it contains useful methods to assess the severity and likelihood of risk through the included measuring scales. The ICO DPIA remains at large high-level, with data controllers carrying the responsibility of determining how the process shall be adjusted to their operation. The German SDM is the most prescriptive out of the three: using the groups from the privacy by design discourse, the SDM determines seven data protection goals that group the principles of Article 5 together with obligations of controllers and data subject rights.

DPIAs are mandatory only when the processing is likely to result in high risk. General criteria of high-risky processing have been given by the WP29, but national DPAs are in the process of further clarifying them through lists of processing activities. So far, eID has been included as a potentially high-risk activity in the ICO list.

Regardless of the obligation under Article 35, a DPIA methodology should be used for the purpose of assessing the appropriateness of data protection by design measures. This is evident not only from the fact that Articles 25 and 35 share common language, but

[502] It is obvious that, where a DPIA has already been performed, the threshold analysis, which is in essence a ‘light’ DPIA, is already covered by the results of the DPIA.

also from looking at the scope of data protection by design as analysed in the previous chapter. Satisfaction of Article 25 is conditioned upon the assessment of the impact of the processing. Even when a DPIA shall not be considered necessary, its threshold analysis (a ‘light’ DPIA) can contextualise the criteria of data protection by design and assess the necessary technical and organisational measures.

The following chapter posits that a threshold analysis should be based on seven data protection goals, motivated by the analysis of Article 35 and the SDM methodology presented. The data protection goals are used to benchmark the data protection by design that can be afforded by eIDAS’ Interoperability Framework.

Chapter 6

Threshold analysis for data protection by design

Taking into account [...] the risks of varying likelihood and severity
for rights and freedoms of natural persons posed by the processing...
— GDPR Art 25(1)

6.1 Introduction

Satisfaction of the principle of data protection by design depends upon the assessment of the risks of the processing to the rights and freedoms of the data subjects. Hence, the technical and organisational measures as part of a data protection by design strategy must be relevant to the result of a threshold analysis.

In this chapter, a threshold analysis methodology is proposed based on the data protection goals of the SDM. The SDM was selected because its seven data protection goals bridge data protection with the concepts and terminology used by the data protection by design scholars.[503] Data protection goals group together the applicable obligations of the GDPR. The groupings assist in identifying corresponding safeguards and measures.

First, the data protection goals are explained, along with how they can be used in the context of data protection by design. Then, the threshold analysis is tailored for the field of eID. Finally, the eID threshold analysis is used to assess the Interoperability Framework.

It is discovered that the current implementation of eIDAS only partially fulfils the goal of unlinkability. In order to assess whether the partial fulfilment is adequate for the

[503] See text of n 348 to n 352.

GDPR, a closer look at the the practical implications, the state-of-the-art and the cost of implementation is needed.

In section 6.2 that follows, the data protection goals from the SDM methodology are explained. The goals form the basis for the creation of a data protection by design methodology in section 6.3. The methodology is then applied on eIDAS' Interoperability Framework in section 6.4. The analysis of section 6.4 reveals that the goal of unlinkability is only partially met within the Interoperability Framework. Section 6.5 argues that the goal of unlinkability has direct consequences on the Interoperability Framework's compliance with data protection by design. Claims of compliance with data protection by design will therefore need to closely examine unlinkability. The material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness*[504] and *Deliverable 5.3: Legal evaluation of the FutureTrust architecture.*[505] Part of the material has been published under *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"*; *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[506]

6.2 Defining Data Protection Goals for a Threshold Analysis

Data protection by design will require the engineering of the data protection principles contained in GDPR Article 5 and thereby the reaching of seven data protection goals as identified by the German Standard Data Protection Model, applying a risk-based approach.[507] As noted in the SDM,

[504] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[505] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 5.3: Legal evaluation of the FutureTrust architecture* (Ref. Ares(2019)4856595 - 25/07/2019, FutureTrust consortium 2019) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_6ee720db94a444b98f1cadafeefca1db.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/ycnogogd⟩).

[506] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (2017) 3(3) The Journal of Web Science 32 DOI: 10.1561/106.00000010; Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

[507] In Martin Rost and Kirsten Bock, *Privacy by Design and the New Protection Goals* (EuroPriSe Whitepaper, 2011) ⟨https://www.european-privacy-seal.eu/AppFile/GetFile/ca6cdc46-d4dd-477d-9172-48ed5f54a99c⟩ accessed 9 February 2019 (archived at ⟨https://tinyurl.com/yazug8th⟩); in International Organization for Standardization, *Information technology – Security techniques – Privacy framework* (ISO:29100:2011, 2011) these are referred to as *"Privacy Principles"* and are mapped against their relevant data protection principles of Dir 95/46/EC.

> *[t]he protection goals Integrity, Availability, Confidentiality, Transparency and Data Minimisation can be found conceptually in the text of the regulation, while also referring to IT security requirements. The protection goals Unlinkability and Intervenability have been adopted as data protection goals in numerous individual articles of the GDPR, inter alia via the principle of purpose limitation, erasure and data portability.*[508]

Hence, a goal can link back to multiple Articles of the GDPR in the same way as a data protection principle can underlie a series of GDPR Articles.

Data minimisation is defined as a basic requirement, whose implementation has a *"sweeping effect on the scope and level of the protection programme defined by the other protection goals."*[509] Data minimisation limits the permissible processing to data that are *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*.[510] Data minimisation presupposes that the principle of *"purpose limitation"* is adhered to, as necessity of the data collection is dependent upon the processing purpose. Minimisation has three dimensions: the amount of data processed, the number of entities to which these data are disclosed to and the extent of the factual control that these entities exercise over the data. Data minimisation is achieved when no or as little as possible data are processed in all three dimensions throughout the entire processing operation. The principle of storage limitation is considered to be a direct consequence of the goal of data minimisation.

Confidentiality refers to the requirement of non-disclosure of certain elements in an ICT system, e.g. input data. Confidentiality of personal data is expressly mentioned in the list of data protection principles in the GDPR. Under the GDPR Article 5(1)(f),

> *personal data shall be... processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").*

GDPR Article 32 on the security of processing also refers to confidentiality. In practice, this implies that personal data shall only be accessed by authorised users.

Integrity requires that data shall remain intact, complete, and up-to-date. This goal mandates safeguards for ensuring the accuracy and completeness of the data. In the field of information security, integrity requires both prevention and detection methods.

[508] Conference of the Independent Data Protection Authorities of the Bund and the Länder, *The Standard Data Protection Model* (v1.0, 2017) 24.
[509] ibid 10.
[510] GDPR (n 371) art 5(1)(c).

While prevention methods mainly rely upon access-control,[511] detection methods relate to the sub-goal of non-repudiation: the provision of irrefutable evidence that an event or action has occurred.[512] In other words, detection methods aim to establish whether the data are trustworthy or not. As aforementioned, GDPR Article 5(1)(f) expressly refers to integrity in its list of data protection principles and shall be conceived as protection *"against accidental loss, destruction or damage"*. GDPR Article 32 also refers to integrity. It is worth noting here that in the SDM there appears to be an overlap between the goal of integrity and the goal of transparency (see further down) as concerns the authenticity of the data. Authenticity is defined as *"the integrity of the link between data and their source"*[513] and while its role is to verify that data are intact by tracing unambiguously to their origin, by retaining information on *"the collection process, its date of expiry and, where appropriate, the identity of the person collecting the data"*[514] and *"the name and revision level of the source data set and a reference to its documentation"*,[515] it also effectuates transparency in the form of *"integrity-assured transparency"*.[516]

Availability refers to the requirement of making data accessible, comprehensible and processable. The aim of availability is to ensure that, provided the goal of confidentiality is satisfied, authorised entities have access to the data in a manner and format suitable for the intended processing.[517] The GDPR lists the goal of availability in Article 32: appropriate technical and organisational measures to ensure the security of processing should include when appropriate *"the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"*.[518]

Unlinkability ensures that an attacker is not able to know if any two or more items of interest in a system are related (for example, an electronic identity with the holder of the eID means).[519] Edge unlinkability, a sub-goal of unlinkability, focuses on the components of the system: when a component at one end of the system cannot link an

[511] *"Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways."* Matt Bishop, *"Introduction to Computer Security"* (Addison-Wesley Professional 2004) 3.

[512] Mina Deng and others, *"A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements"* (2011) 16(1) Requirements Engineering 3 doi: 10.1007/s00766-010-0115-7, 8.

[513] *The Standard Data Protection Model* (n 508) 14.

[514] ibid 14.

[515] ibid 14.

[516] ibid 14.

[517] Marit Hansen, Meiko Jensen, and Martin Rost, *"Protection Goals for Privacy Engineering"* (2015 IEEE Security and Privacy Workshops, San Jose, CA, May 2015) doi: 10.1109/SPW.2015.13 160.

[518] Which, in fact, encompasses all three of the principles: *"[T]he ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"* GDPR (n 371) art 32(b).

[519] *"[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system"*: International Organization for Standardization, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model* (ISO/IEC 15408-1, 2009) 78.

action to any other components of the system, edge unlinkability is met.[520] In broad terms, unlinkability methods aim to hide the link between two actions, whether the actions correspond to uses, identities or pieces of data. Unlinkability, in other words, refers to controls against the aggregation of sources. For example, aggregation of data sets has been shown to reverse data pseudonymisation and enable profiling.[521] Unlinkability is not expressly referred to in the GDPR. However, unlinkability plays a key role in data protection, as a requirement to satisfy the principles of data minimisation and purpose limitation.

As aforementioned, data minimisation requires the processing (including the collection) of only the data *"limited to what is necessary"*[522] to accomplish a certain purpose. Under the purpose limitation principle, processing purposes must be specified, explicit and legitimate;[523] consequently purposes shall already be defined before data collection. Therefore, not only collection of data must be limited, but collected data must be strictly necessary to a predefined relevant purpose. In this context, unlinkability refers to the risk of linking personal information to its data subject, for example by aggregating identifiers to build a profile of the user, potentially threatening both data minimisation and purpose limitation. Additionally, although unlinkability is usually defined in respect to an outside (malicious) attacker,[524] in a data protection context it applies equally to outside and inside actors[525] – in other words, linkability as a data protection risk could be the result of an accidental linkage of data by actors or processes within the system assuming that linkage is not necessary for the processing purpose at stake. Therefore, the overarching goal of unlinkability is to eliminate risks of data misuse by minimising risks of profiling.[526] To achieve this, this goal serves three related functions: to separate

[520] Andreas Pfitzmann and Marit Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology* (v0.33, 2010) ⟨https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.doc⟩ accessed 12 June 2015 (archived at ⟨https://tinyurl.com/ycshm2ey⟩) 12.

[521] Perhaps the most well-known case is the de-anonymisation of AOL user data by their aggregation with publicly-sourced data: Michael Barbaro and Tom Zeller Jr, *"A Face Is Exposed for AOL Searcher No. 4417749" The New York Times* (New York, 6 August 2006) ⟨https://www.nytimes.com/2006/08/09/technology/09aol.html⟩ accessed 5 January 2020 (archived at ⟨http://archive.ph/QeAuG⟩) ; similar techniques have been successfully applied to anonymised web browsing data: Jessica Su and others, *"De-Anonymizing Web Browsing Data with Social Networks"* [2017] Proceedings of the 26th International Conference on World Wide Web WWW '17 1261 DOI: 10.1145/3038912.3052714.

[522] GDPR (n 371) art 5(1)(c).

[523] ibid art 5(1)(b).

[524] Myrto Arapinis and others, *"Analysing Unlinkability and Anonymity Using the Applied Pi Calculus"* (2010 23rd IEEE Computer Security Foundations Symposium, 17–19 July 2010) DOI: 10.1109/CSF.2010.15 107. See also Pfitzmann and Hansen (n 520) fn. 10*"'Attacker' is the historical name of the set of entities working against some protection goal like anonymity."*; A Cooper and others, *Privacy Considerations for Internet Protocols* (RFC 6973, 2013) DOI: 10.17487/RFC6973 10–11.

[525] Meilof Veeningen, Benne de Weger, and Nicola Zannone, *"Data minimisation in communication protocols: a formal analysis framework and application to identity management"* (2014) 13(6) International Journal of Information Security 529 DOI: 10.1007/s10207-014-0235-z, 530.

[526] Harald Zwingelberg and Marit Hansen, *"Privacy Protection Goals and Their Implications for eID Systems"* (Jan Camenisch and others eds, Springer Berlin Heidelberg 2012) DOI: 10.1007/978-3-642-31668-5_19 247: *"The overarching objective of this protection goal is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and potentially violating the purpose limitations related to the data."*

data from persons; to separate data collected for different purposes; and to separate personal data between different domains.[527]

Transparency, as a goal, refers to the necessity of making sure all involved parties are able to comprehend *"the legal, technical, and organisational conditions setting the scope for th[e] processing".*[528] It covers 'soft' privacy – requiring the adoption of privacy policies, and the putting in place of reporting and auditing mechanisms. In the GDPR, the transparency principle is listed in Article 5(1)(a), which requires personal data shall be processed *"lawfully, fairly and* ***in a transparent manner*** *in relation to a data subject"* [emphasis given]. Transparency obligations can be found in Articles 12–14.[529] Compliance with the transparency principle requires both preventative and corrective measures to be implemented both before and after a potential data breach. Article 15 and the right to access could also be seen as a transparency guarantee.

Intervenability aims to ensure that parties to a data processing activity can intervene on the processing activity when needed. In the GDPR intervenabilty is achieved through the provisions relating to data subject rights (Articles 15–22, namely the right to access, rectification, erasure, access, objection and portability). Intervenability in a wider sense covers measures implemented by controllers to control the activities of their data processors, or their technical infrastructure.[530] The principle of accountability introduced by GDPR Article 5(2) could be seen as being captured by both the goal of transparency (the data controller shall generate records of processing activities in order to demonstrate compliance) and the goal of intervenability (the data controller shall be able to intervene in order to adapt processing activities).

Of note, the pursuance of the foregoing data protection goals implies the putting in place of both organisational and technical measures, such as tailored policies and infrastructure or architecture. Therefore, a data protection by design approach covers both a *"data protection-by-policy"* and *"data protection-by-architecture"* approach.[531]

The seven data protection goals detailed in the SDM map data protection requirements to control measures. As such, the SDM offers a very useful tool to demonstrate compliance with the principle of data protection by design. The goals also appear in several

[527] Zwingelberg and Hansen (n 526) 247.
[528] ibid 247.
[529] In relation to data subjects' rights as defined in GDPR Arts. 13–14, 15–22 and 34: Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (WP 260, 2017) 5.
[530] Zwingelberg and Hansen (n 526) 247.
[531] Sarah Spiekermann and Lorrie Faith Cranor, *"Engineering Privacy"* (2009) 35(1) IEEE Transactions on Software Engineering 67 doi: 10.1109/TSE.2008.88, 68.

methodologies,[532] although not always with those names.[533]

Because by definition the principle of data protection by design remains high-level (essentially referring back to GDPR Article 5), a process is needed to select in context the means to achieve these goals. A DPIA is a process, the purpose of which is to assess prior to the beginning of the processing *"the impact of the envisaged processing operations on the protection of personal data"* as per GDPR Article 35. As the output of such a process should be regularly reviewed, in particular *"when there is a change of the risk represented by processing operations,"*[534] a DPIA should be conceived as an iterative process. Because a DPIA shall include

> *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*[535]

after an assessment of the risks to the rights and freedoms of data subjects created by the processing, it should guide or support the data protection by design choices made by data controllers at the time at which processing means are evaluated. Because some details of the processing are not expected or cannot be known as early as the design stage, the assessment detailed here can start off as a threshold analysis (i.e. a 'light' DPIA), assessing the envisaged processing against expected safeguard. In further iterations during the life-cycle of the system, the threshold analysis can be extended to a full DPIA if the threshold for processing likely to result in high-risk is reached. In any case, a DPIA methodology should be seen as a process to effectuate data protection by design.

Breaking down the requirements into data protection goals facilitates the identification of important or potentially problematic areas of risk and permits the alignment of identified or expected risks to the catalogues of counter-measures.[536] The SDM methodology should therefore be considered as a key component of a data protection by design methodology.

[532] Felix Bieker and others, *"A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation"* in Stefan Schiffner and others, *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016) DOI: 10.1007/978-3-319-44760-5_2; *The Standard Data Protection Model* (n 508). Also in Pfitzmann and Hansen (n 520); Rost and Bock (n 507); Zwingelberg and Hansen (n 526).

[533] For example, in LIND(D)UN, mentioned in n 536, the goals of confidentiality, unlinkability, intervenability and transparency appear as confidentiality goals (covering both confidentiality and unlinkability), control goals and practice goals: Hansen, Jensen, and Rost (n 517) 164.

[534] GDPR (n 371) art 35(11).

[535] International Organization for Standardization, *Information technology – Security techniques – Guidelines for privacy impact assessment* (ISO/IEC 29134:2017, 2017) vi.

[536] A catalogue of measures is planned for the Standard Data Protection Model, but has not yet been made available in the English version. See *The Standard Data Protection Model* (n 508) 46. However, alternative catalogues of safeguards exist as separate instruments, as is for example the privacy threat modelling methodology LIND(D)UN: Kim Wuyts and Wouter Joosen, *LINDDUN privacy threat modeling: Privacy knowledge (tables)* (Technical Report (CW Reports), Department of Computer Science, KU Leuven 2015) ⟨https://linddun.org/downloads/LINDDUN_tables.pdf⟩ accessed 25 April 2018.

6.3 A Data Protection by Design Methodology for eID Schemes

A threshold analysis, assessing whether eID schemes and their operation within the Interoperability Framework meets the criteria of the data protection goals, allows to draw important conclusions regarding data protection by design: First, it provides for a process to identify potential risks that the processing for the purposes of eID will pose upon the data subjects; second, it allows the determination of organisational and technical controls to safeguard the data protection goals. At a later stage, when the eID scheme is in operation, this data protection by design methodology can be expanded to a full DPIA that will ensure the continued monitoring of risk levels.

As aforementioned, in order to identify risks, the first step is to describe and map the data flows. In the lifecycle of an eID scheme, several operations can be observed. The main operation is of course the enrolment of new users and the (subsequent) authentication of eID credentials against Service Providers. At the same time, though, complementary operations need to be performed: The creation and management of a 'history function', that can be used either as a personal log of a user's activities or as an audit trail for errors or incidents; a process for access and rectification of information stored on the eID means, either because they were mistakenly registered or because the circumstances of the user changed (for example, a change of address); a process for the revocation and renewal of eID credentials, in cases where the credentials have been compromised or expired; and finally a process for the termination of the eID scheme, for example when an eID scheme is being replaced by a newer scheme or where multiple eID schemes exist and a user wishes to transfer their eID credentials. The data protection goals should be met for all these operations. Notably, eIDAS high level and more technical requirements (in particular within implementation acts) can be organised in relation to the same data protection goals as per table 6.1. In this sense, eIDAS could be seen as complementing the GDPR.

	Data minimisation	Availability	Integrity	Confidentiality	Unlinkability	Transparency	Intervenability

GDPR	5(1)(c);
	5(1)(e);
	25; 32;
		5(1)(e);
		13; 15; 20;
		25; 32;
			5(1)(f);
			25; 32; 33;
				5(1)(f);
				25; 28(3)(b);
				29; 32;
					5(1)(c);
					5(1)(e); 17;
					22; 25; 40(2)(d);
						5(1)(a);
						13; 14; 15; 19;
						25; 30; 32; 33;
						40; 42;
							5(1)(d);
							5(1)(f); 13(2)(c);
							14(2)(d); 15(1)(e);
							16; 17; 18; 20;
							21; 25; 32;

eIDAS	5(2);
	Impl Reg 2015/1501
	6(2) and 9(3);
	Impl Reg 2015/1501
	ANNEX
	I
		7(f);
		11(1);
		Impl Reg 2015/1502
		ANNEX
		2.4.6;
			12(3)(c);
			Impl Reg 2015/1501
			10;
			Impl Reg 2015/1502
			ANNEX
			2.3.1, 2.4.6
				12(3)(c);
				Impl Reg 2015/1501
				6(1);
				Impl Reg 2015/1502
				ANNEX
				2.4.6;
					5(2);
					12(3)(c);
						Impl Reg 2015/1502
						ANNEX
						2.4.2;
							—

Table 6.1: Allocation of GDPR and eIDAS articles per Data Protection Goal

Data minimisation, as already stated, is one key overarching goal. In the context of eID schemes, its importance can be illustrated by the evolution of scheme architectures – centralised configurations, where all personal information was stored in a singular database, are replaced with federated decentralised models, which allow for the separation of data into smaller detached storage locations. Data minimisation, when considering eID schemes, can have three different dimensions: minimisation of content, under which the amount of information processed should not go beyond what is necessary for the specific purpose at stake;[537] temporal minimisation, under which information should be processed only for the minimum amount of time necessary for the specific purpose;[538] minimisation of scope, where data should be processed only for the specific purposes identified beforehand.[539] The three dimensions relate to different data protection principles which should be seen as being complementary. Minimisation of content refers to the definition of data minimisation as given by the GDPR, in other words as a specification of the general principle of proportionality. Under minimisation of content a service wishing to authenticate a user should ask only for the identifiers that are necessary for the needs of the service. Temporal minimisation, on the other hand, refers to the GDPR's 'storage limitation' principle. In this sense, data are minimised because sets that have become unnecessary for the purposes of the service are destroyed or anonymised. Minimisation of scope operationalises purpose limitation,[540] i.e. that data collected will not be used in further processing that is incompatible to the original purpose. Minimisation of content can be illustrated through an example: During the STORK project, a service offering pseudonymous chat rooms for minors in Austria was piloted.[541] The objective, therefore, of the service was to verify that users were within a certain age range; the identity of the user was not important. Essential content, therefore, for successful authentication of the user was their age. As regards temporal minimisation, no data needed to be stored for the purpose of the service.[542] Minimisation of scope, in this example, is the result of content and temporal minimisation: Since the only attribute communicated is an attestation of age and this attribute is not stored, further processing for purposes other than access to the chat room is not possible.

Confidentiality refers to access and disclosure of personal data only by authorised entities. In other words, all personal data have to be protected against unauthorised access.[543] For eID provision, the protection should cover the identity information (i.e. the identifiers stored in the eID means and the eID credentials) when the identity data are at rest (i.e. in storage with the Identity Provider or the Service Provider). Additionally, the same protection should be warranted to data in transit: aside from the identifying information, this includes traffic data (i.e. the metadata) which should be protected

[537] GDPR (n 371) art 5(1)(c): *"limited to what is necessary in relation to the purposes"*.

[538] ibid art 5(1)(e): *"for no longer than is necessary for the purposes for which the personal data are processed"*.

[539] ibid art 5(1)(b): *"not further processed in a manner that is incompatible with those purposes"*.

[540] As opposed to purpose limitation in a wider sense, which refers to the existence of an explicit and legitimate purpose for data to be collected: Lukas Feiler, Nikolaus Forgó, and Michaela Weigl, *"The EU General Data Protection Regulation (GDPR): A Commentary"* (Globe Law and Business 2018) 18.

[541] Herbert Leitold, *"Challenges of eID Interoperability: The STORK Project"* (Privacy and Identity Management for Life, 2011, Springer Berlin Heidelberg) 138.

[542] Note that this does not consider any auditing or crime prevention requirements (e.g. keeping logs of IP addresses or content of the chats).

[543] GDPR (n 371) art 5(1)(f).

against third parties that wish to monitor the communications. If the scheme offers its users the ability to review past transactions ('history function'), this function should be available only to the holder of the eID means, whereas any activity logs for security purposes should be accessed only by authorised auditors and competent authorities in the event of a security or data breach. Access to the identity data for rectification or erasure should be granted only to the data controller and/or the holder of the eID means after successful authentication of their identity. Whether a credential has been revoked or not should be disclosed only after authorisation of the inquiring party. Finally, in the event of a migration to a different scheme, personal data have to stay protected against unauthorised access, whereas after successful migration or termination of the scheme all personal data should be deleted. Traditional measures for ensuring confidentiality include access control and encryption measures.[544]

Integrity during the enrolment process is served by the verification of the provided information against authoritative sources. The verification, and the resulting level of certainty about the validity of the information, varies depending on the national scheme.[545] The correct verification of identity data guarantees the integrity of the eID means used during eID provision, since the data have been deemed verified according to the issuing entity. Entries must not be modified by unauthorised entities, unless after the eID holder's explicit permission. Any edits to the entries should be performed by the issuing entity, after request of the eID holder. Revoked credentials must not be able to be used after their revocation. If pseudonyms are being used, it is important that they are marked as such and only the holder of the eID means can claim to be holder of the pseudonym. Any compromise to the integrity of the data should be promptly communicated to the interested parties.[546] Safeguards for integrity vary from legal controls[547] (at least for validity checks of the authoritative sources during issuance) to integrity checks of computer systems[548] and comparison of hash values of data,[549] as well as the creation of secure logs.[550]

Availability must always be viewed in parallel to the protection goal of confidentiality, i.e. the scheme must ensure that data are available to authorised entities. The data should also be available to the data controller and/or the holder of the eID means in case a rectification is needed. In the event of a revocation of the eID means, the revocation

[544] GDPR (n 371) art 32; Bieker and others (n 532) 33; CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf⟩ accessed 25 May 2019 14–17 and 24–28; Wuyts and Joosen, *LINDDUN privacy threat modeling* (n 536) 6.

[545] For example, in the national scheme of Austria verification is performed against population registers, in Germany from the Ministry of the Interior; in the UK verification is performed against the Passport Office and the Driver and Vehicle Licensing Agency. See chapter 8.

[546] GDPR (n 371) art 33.

[547] Bieker and others (n 532) 33.

[548] ibid 33.

[549] Bieker and others (n 532) 33; CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 544) 21–23.

[550] Wuyts and Joosen, *LINDDUN privacy threat modeling* (n 536) 6.

must be performed within a set timeframe; if the revocation is accompanied with a renewal of the means, the new eID means should be available before the revocation of the previous means. There must not be a time where neither the old nor the new means work. Availability also covers the provision of the information of GDPR Article 15 to the holder of the eID means, upon their request. Mitigating safeguards for availability include, inter alia, regular back-ups (redundancy)[551] and secure logs.[552]

Transparency refers to the eID data transmitted during an authentication. It also refers to the information provided to the holder of the eID means, not only about the eID data but also about the involved entities in the transaction. This translates into two sets of information: on the one hand, the holder must be able to check which data will be transmitted before their transmission; on the other, the relying parties to the transaction (i.e. the service providers) should provide information about their identity to the user – ideally in a mutual authentication. Privacy policies and terms of use also fall within this protection goal. Thus, controls for transparency are measures for documentation and logging[553] as well as mutual authentication of Service Providers.

Intervenability relates to GDPR's provisions on data rectification[554] and goes beyond. In eID schemes, rectification can refer not only to the identity data (i.e. the correctness of a date of birth or address) but also to the outcome of an authentication: if the eID holder believes that an authentication has not yielded the correct result, they should be able to intervene to confirm the accuracy of the identity data. The option to erase the identity data, or part of the data, is also considered part of intervenability.[555] A flip side of this is the ability to challenge a revocation of the eID means, in cases where the holder believes the means has been revoked wrongfully. As such, rectification is ensured mainly through organisational measures: Information and rectification procedures,[556] single points of contact.[557]

Unlinkability as a goal is intimately related to the data minimisation and purpose limitation principles. The aim of unlinkability for eID schemes is to avert third parties from getting insight or from learning about the interactions of parties to a transaction. Additionally, unlinkability refers to the minimisation of the knowledge and the ability to accumulate data about the holder of an eID that parties to a transaction (i.e. the service providers) have. The service providers should not be able to link separate transactions together, or infer that they refer to the same eID holder. To satisfy this aim, a minimisation of the disclosed data must be performed. Several complementing

[551] Bieker and others (n 532) 33; CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 544) 78–79.

[552] CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 544) 71–72.

[553] Bieker and others (n 532) 33; CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 544) 37–38.

[554] GDPR (n 371) art 16.

[555] ibid art 17.

[556] Bieker and others (n 532) 33; CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (n 544) 35–38.

[557] Bieker and others (n 532) 33.

controls exist to effectuate unlinkability: data avoidance, separation of contexts through federated distribution, encryption, access control, anonymisation, data destruction etc.[558]

A growing body of literature identifies two primary requirements to reach unlinkability in eID schemes: minimisation of the amount of information disclosed by the scheme; and masking the different pieces of information disclosed to prevent linking.[559] Minimisation of the disclosed information is served by the method of selective disclosure. Selective disclosure refers to the ability to granularly release information for a specific purpose. Selective-disclosure-capable schemes have the ability to accept and transmit only a subset of the available attributes, depending on the processing at hand.[560] Depending on scheme architecture, selective disclosure can be implemented at user level, where users select attributes to be transmitted, but also at service level, where each service (for example an eID provider) only transmits the attributes required for a certain use. On the other hand, masking of information is performed through pseudonymisation. Pseudonyms can be deployed in two ways: In some implementations, different pseudonyms are constructed for every pair of 'Service Provider ⟷ user.' This way no two Service Providers receive the same pseudonym. In contrast, in other deployments pseudonyms change from use to use even for the same Service Provider. A Service Provider is not able to distinguish that two uses concern the same user.[561] Selective disclosure and pseudonymisation therefore appear as essential conditions to satisfy unlinkability. Importantly, the two measures are interdependent: inclusion of pseudonyms in a dataset will not result in unlinkability if the rest of the identifying information in the dataset enable linkages, e.g. when it remains stable. Pseudonymity is effective when

> *the less personal data of the pseudonym holder can be linked to the pseudonym; the less often and the less context-spanning pseudonyms are used and therefore the less data about the holder can be linked; the more often independently chosen pseudonyms are used for new actions (i.e., making them, from an observer's perspective, unlinkable).*[562]

A list of example safeguards discussed in this section, per data protection goal, can be seen in table 6.2.[563]

[558] George Danezis and others, *Privacy and Data Protection by Design – from policy to engineering* (ENISA report, 2014) DOI: 10.2824/38623 7.

[559] Pfitzmann and Hansen (n 520) 14–16 and 21–23; Zwingelberg and Hansen (n 526) 6–7; Veeningen, Weger, and Zannone (n 525) 537–538.

[560] Armen Khatchatourov, Maryline Laurent, and Claire Levallois-Barth, *"Privacy in Digital Identity Systems: Models, Assessment, and User Adoption"* in Efthimios Tambouris and others (eds), *14th International Conference on Electronic Government (EGOV), Aug 2015, Thessaloniki, Greece* (Lecture Notes in Computer Science, Springer International Publishing July 2015) vol LNCS-9248 DOI: 10.1007/978-3-319-22479-4_21, 2.

[561] George OM Yee, *"Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards"* (IGI Publishing 2011) 42.

[562] Cooper and others (n 524) 10.

[563] Bieker and others (n 532) Table 1.

Protection goal	Component	Measure
Availability	Data, systems, processes	Redundancy, protection, repair strategies
Integrity	Data	Comparing hash values, integrity monitoring
	Systems	Limitation of write permissions, regular integrity checks, clamping down on malicious software
	Processes	Setting references values (min/max), control of regulation
Confidentiality	Data	Encryption, data partitioning
	Systems	Physical access control
	Processes	Logical access control
Unlinkability	Data	Anonymity, pseudonymity, attribute-based credentials
	Systems	Separation (isolation) of stored data, systems and processes
	Processes	Identity management, anonymity infrastructures, audits
Transparency	Data	Documentation, logging, archiving
	Systems	System documentation, logging of configuration changes
	Processes	Documentation of procedures, logging
Intervenability	Data	Access of data subjects to their data (information, rectification, blocking, deletion)
	Systems	Off-switch
	Processes	Helpdesk/single point of contact for modification/deletion, change management

Table 6.2: Example controls per data protection goal

6.4 Assessing the Data Protection by Design Within the Interoperability Framework

The Interoperability Framework is meant to extend the reach of national eID schemes across borders. In order to allow interoperability of the different architectures, the Interoperability Framework introduces common specifications that participating schemes shall support. Much of the specifications governing the Interoperability Framework come in the form of implementing acts and technical specifications.

Looking at the Interoperability Framework through the prism of data protection goals, it is clear that those goals have guided the action of the EU legislature. It is arguable however whether unlinkability has been satisfactorily met.

As regards DATA MINIMISATION, eIDAS defines a common Minimum Dataset of identifiers for natural and legal persons.[564] The goal of the Minimum Dataset is to define the absolute minimum number of attributes necessary to *"uniquely representing a natural or legal person"*.[565] The premise is that these attributes shall be enough to uniquely identify a person against Service Providers across all Member States. Therefore, although

[564] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1, ANNEX..

[565] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73, art 12(4)(d).

additional attributes may be supported, they are not specified in eIDAS.[566] Additionally, the eIDAS nodes are prohibited from storing any personal data,[567] apart from those required in order to, *"in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident."*[568] However, the data shall be stored *"for a period of time in accordance with national requirements"*[569] and the minimum required elements are the node's identification, the message identification and the message's date and time.[570]

A series of provisions in the Implementation Acts aim to satisfy the goal of CONFIDENTIALITY, by guarding against unauthorised access and disclosure to personal data. The release of person identification data has to be preceded by *"reliable verification of the electronic identification means"*[571] and when at rest identification data shall be protected against unauthorised access through *"implement[ed] security controls"*.[572] A prior check as to the validity of the eID means is also required.[573] Although the exact security controls are not defined, the approach is risk-based with higher Levels of Assurance requiring higher security guarantees.[574] When in transit, only electronic communication channels protected against *"eavesdropping, manipulation and replay"*[575] are used and *"sensitive cryptographic material" "is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text."*[576]

The goal of integrity is mainly served by the definition of the LoAs. The three levels, *"Low"* – *"Substantial"* – *"High"*, relate to three varying degrees of certainty that three conditions are met: that the holder of an eID means is in possession of the claimed identity the eID means verify; that the claimed identity the eID means verify is genuine; and that the holder of an eID means and the owner of the identity the eID means verify are one and the same.[577] Integrity is approached again in a risk-based manner.

[566] eIDAS Technical Sub-group, *eIDAS SAML Message Format* (v 1.1.2, 2016) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_message_format_v1.0.pdf?version=1&modificationDate=1497252920416&api=v2⟩ accessed 4 November 2019 (archived at ⟨https://tinyurl.com/y6u2qnds⟩) para 5: *"Exchange of further additional attributes between eIDAS-Connector and eIDAS-Service MAY be supported. Additional attribute definitions are out-of-scope of this specification and of [eIDAS-AttrProfile]."*

[567] Impl Reg 2015/1501 (n 564) art 6(2).

[568] ibid art 9(3).

[569] ibid art 6(2).

[570] ibid art 6(2): *"The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements: (a) node's identification; (b) message identification. (c) message date and time."*

[571] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/7, ANNEX 2.3.1.

[572] ibid ANNEX 2.3.1.

[573] ibid ANNEX 2.3.1.

[574] Level *"Low"* has to be secured against attacks of *"enhanced-basic potential"*; level *"Substantial"* against *"moderate"* attacks; level *"High"* against *"high"* attacks: ibid ANNEX 2.3.1.

[575] ibid ANNEX 2.4.6.

[576] ibid ANNEX 2.4.6.

[577] ibid ANNEX 2.1.2.

For the level *"Low"* only the assumption that the three statements above hold true is enough,[578] whereas for the level *"Substantial"* a verification of the statements must have happened and for level *"High"* the identity evidence have to be supported through photo or biometric evidence.[579] Renewal of the eID means has to match the same assurance requirements[580] and suspension, revocation and reactivation can only be performed by authorised entities.[581] Integrity should be secured through technical controls.[582]

Availability is first and foremost set in the text of eIDAS. Article 7(f) sets the *"availability of authentication online"* as a pre-condition for notification of the scheme to the Commission in order to participate in the Interoperability Framework, which the Member State has to guarantee. In fact, if the authentication operation becomes unavailable, the notifying Member State and the operator of the scheme bear the liability for any damages caused to natural or legal persons.[583] Thus availability is ensured firstly through a legal control. Additionally, *"availability of the information processed"* must be protected through security controls, although the Implementing Act does not specify specific measures.[584] Relevant information about the registration, revocation and management of eID means shall be kept in *"an effective record-management system"*,[585] taking into account data protection and data retention legislation.

eIDAS does not allow for authentication of the Service Providers, before they are allowed to request eID data. The xml schema when Service Providers are communicating with eIDAS nodes should include information about the Service Provider in the metadata,[586] and an indication whether they are a public or private sector body must be present.[587] However, this information is not required to be displayed to the user. Equally, there is no requirement to display which attributes are asserted before transmission of the eID data. Member States and Service Providers have the discretion to implement a user interface

[578] ibid ANNEX 2.1.2: *"1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same." Note though that national schemes that support the level 'Low' are only voluntarily recognised by electronic services of other Member States: eIDAS (n 565) art 6(2)".*

[579] Impl Reg 2015/1502 (n 571) ANNEX 2.1.2.

[580] ibid ANNEX 2.2.4.

[581] ibid ANNEX 2.2.3.

[582] ibid ANNEX 2.4.6.

[583] eIDAS (n 565) arts 11(1), 11(3).

[584] Impl Reg 2015/1502 (n 571) ANNEX 2.4.6.

[585] ibid ANNEX 2.4.4.

[586] eIDAS Technical Sub-group, *eIDAS SAML Message Format* (n 566) para 2: *"Human readable information of the organization operating the eIDAS-Node SHOULD be indicated by the ⟨md:Organization⟩ element. At least the elements ⟨md:OrganizationName⟩, ⟨md:OrganizationDisplayName⟩, and ⟨md:OrganizationURL⟩ SHOULD be provided."*

[587] Through the defined element ⟨eidas:SPType⟩: ibid para 5.

that displays them.[588] Transparency is addressed by way of published notices and user information about the Service Providers and the national scheme.[589]

Intervenability relates to the user rights in the Interoperability Framework to rectify, revoke or erase their eID data. However, since the Interoperability Framework only relays information from national schemes to Service Providers, these procedures should be dealt with individually by procedures set up in the national schemes and services. As such, intervenability measures are out of the scope of eIDAS and its Implementing Acts. As a result, intervenability is provisioned solely through the GDPR.

Unlinkability appears to be one of the most challenging goals to meet in the context of the Interoperability Framework. As aforementioned, unlinkability can be facilitated through selective disclosure and pseudonymisation. While eIDAS does not preclude the use of pseudonyms,[590] the systematic transmission of the Minimum Dataset severely limits their usefulness. Since the mandatory attributes of the Minimum Dataset[591] are present in all authentications, it is not possible to implement selective disclosure for services that require less attributes than those in the Minimum Dataset.[592] Additionally the existence of the *"uniqueness identifier"* precludes any meaningful use of pseudonyms, since even in the case of substitution of the identifier with a pseudonym, this pseudonym will have to *"remain unchanged for the lifetime of the account"*.[593] As a result, in practice even a pseudo-random value will function as an *ad-hoc* permanent unique identifier, thereby increasing the risk of linkability between datasets or between transactions.

[588] The guidance specifies that this might be useful for the purposes of consent: eIDAS Technical Sub-group, *eIDAS SAML Message Format* (n 566) para 23.

[589] Impl Reg 2015/1502 (n 571) ANNEX 2.4.2: *"1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy. 2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service. 3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information."*

[590] eIDAS (n 565) art 5(2).

[591] Current family name, current first name, date of birth and uniqueness identifier.

[592] See also the concerns raised by Marko Hölbl, *CEPIS – Position on the Electronic Identification and trust services (eIDAS)* (LSI SIN(15)01 v1.3, 2015) ⟨http://www.cepis.org/media/Position%20on%20the%20Electronic%20identification%20and%20trust%20services%20(eIDAS).pdf⟩ accessed 23 June 2019 (archived at ⟨https://tinyurl.com/yak94paz⟩) 3: *"The focus on identification and the requirement that the link to the person be unambiguous, together with the centralised verification architecture, makes it hard to imagine solutions that allow authentication with only the attributes necessary for the transaction or that enable pseudonymous use. [...] The possibility of implementing such functionality is not excluded by the eIDAS Regulation, but neither is it implied and therefore may be overlooked."*

[593] eIDAS Technical Sub-group, *eIDAS SAML Attribute Profile* (v. 1.1.2, 2016) ⟨https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf⟩ accessed 4 November 2016 (archived at ⟨http://archive.fo/pLWy5⟩) 23.

6.5 The Partially Met Goal of Unlinkability

Based on the analysis in section 6.4, it can be asserted that the current implementation of eIDAS seems to take into account most of the data protection goals. However, three goals appear problematic: Transparency, intervenability and unlinkability. As explained above, mutual authentication between the Service Provider and the user has not been implemented in the Interoperability Framework. The identification and authentication processes that take place are built on the trust of the information that the Service Provider includes in the metadata. It is arguable whether leaving the decision to display this information to the user up to the discretion of the national schemes is the best way to serve transparency. Besides, allowing users to see which attributes are transmitted would also assist in enhancing intervenability. It should be noted, though, that the Interoperability Framework was intended to facilitate the functionalities of national eID schemes, not to add new functionalities. In this respect, although facilitation of transparency and intervenability could certainly be improved, at least the Interoperability Framework offers a way for national eID schemes to provide such information if they so wish through the inclusion of optional metadata.

On the contrary, facilitation of unlinkability is inherently limited. The Interoperability Framework seems to be quite restrictive in terms of unlinkability, with the main obstacles being the Minimum Dataset and the limited use of pseudonyms. As it appears from the description of the LoAs and their corresponding data protection goals, i.e. INTEGRITY, Member States are in no position to refuse interoperability to schemes of a ‘Substantial’ or ‘High’ LoA. Consequently, national schemes that have been designed to offer a high level of unlinkability[594] may be requested to accept lower levels when interoperating within the Interoperability Framework. It is doubtful, therefore, whether the Interoperability Framework can claim to comply with data protection by design. Indeed, under GDPR Article 25(1), a positive answer to this question will rely on a qualification of the ‘appropriateness’ of the level of unlinkability supported by the Interoperability Framework via the state of the art, the nature of processing (including the particularities of the participating national schemes and services) and the cost of implementation. The goal of unlinkability and its consequences for the Interoperability Framework are further clarified in the next chapter.

6.6 Conclusion

A threshold analysis based on data protection goals is useful in order to identify the areas where eIDAS has provided safeguards and any areas where the safeguards proposed might not be adequate. As has been demonstrated, the eIDAS Interoperability Framework has

[594] See the analysis of national implementations in chapter 8.

been set up with most of the protection goals in mind. However, the goals of transparency, intervenability and unlinkability are only partially met.

In terms of transparency and intervenability, an authentication of the Service Provider to the user so that the latter has proof of the Provider's identity would build up trust and allow the users to exercise their rights more effectively. Accordingly, displaying to the users which attributes are being transmitted would also boast transparency and intevenability for the same reasons. A means for Service Providers to provide such information has been implemented, but it not mandatory or on by default and it relies on the discretion of the national scheme.

Unlinkability, on the other hand, is met by a definition of a strict number of attributes allowed in the Minimum Dataset (as a data minimisation measure) and a non-prohibition clause as to the use of pseudonyms. However, albeit minimal, the mandatory presence of attributes regardless of recipient puts constrains on the selective disclosure supported by the Interoperability Framework. And, besides, the presence of a unique identifier challenges the usefulness of pseudonyms.

Hence, there is a question as to how well the Interoperability Framework can facilitate data protection by design and therefore satisfy Article 12(3)(c) of eIDAS. The next chapter looks at the goal of unlinkability and its relationship with pseudonymisation and selective disclosure. It examines the prescription of pseudonymisation under the GDPR and explains why pseudonymisation can only be achieved if coupled with selective disclosure. Next, it analyses how the Interoperability Framework supports pseudonymisation and selective disclosure.

Chapter 7

Unlinkability under the eIDAS Interoperability Framework

...implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation...
— GDPR Art 25

7.1 Introduction

The goal of unlinkability is only partially met by the eIDAS Interoperability Framework. This is mainly because of the strict definition of the Minimum Dataset and its unique identifier. In particular, there is a question whether unlinkability can be satisfied when effective pseudonymisation of datasets is not possible.

This chapter looks into the way pseudonymisation can work within the Interoperability Framework. It first explains why the key enabler of unlinkability, pseudonymisation, cannot exist without the ability to selectively transmit attributes, i.e. selective disclosure. It justifies this argument based on the definition of pseudonymisation under the GDPR explaining the practical implications of the absence of selective disclosure.

It then examines the Interoperability Framework and its technical specifications. It is confirmed that the existence of a mandatory set of attributes within the Minimum Dataset, although conceived to satisfy data minimisation, in fact precludes participating schemes effectuating selective disclosure. The non-discrimination clause for the use of pseudonyms in eIDAS Article 5(2) is in practice of no use, since effective pseudonymisation is only possible if coupled with selective disclosure.

The chapter concludes that the absence of selective disclosure and the ineffective pseudonymisation can in fact lower the level of data protection by design of those schemes that rely on a high unlinkability level. Such a result would be permissible only if justified against the state of the art, the nature of processing and the cost of implementation.

Section 7.2 presents the way pseudonymisation is formulated in the GDPR and explains why selective disclosure is a key requirement for effective pseudonymisation for eID. Section 7.3 examines the implementation of pseudonymisation by the Interoperability Framework and discusses the limits it places on unlinkability. It concludes that such limits must be justified according to the contextual factors of Article 25. Of note, the material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness*[595] and published under *"What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation"*[596] and *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[597]

7.2 The Concept of Pseudonymisation under the GDPR

Pseudonymisation in the GDPR is conceived as a means to implement the principle of data minimisation and thereby the principle of data protection by design as per Article 25. In Article 4(5), the GDPR includes – for the first time – a definition for pseudonymisation:

> *"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

[595] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[596] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation"* (Detlef Hühnlein and others eds, Open Identity Summit, 15 September 2016, Rome, Italy, 2016) vol P-264 ⟨https://dl.gi.de/handle/20.500.12116/598⟩ accessed 12 January 2019.

[597] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

Notably, pseudonymised data are not exempt from the GDPR. Although pseudonymisation is accepted as reducing the risks of processing,[598] pseudonymised data are still considered to include information that can render a person identified or identifiable.[599] The practical implication of the obligation to keep *"such additional information"* separate means that in order to achieve pseudonymisation under the GDPR's definition any attribution of information to identifiable persons should be excluded.

In the field of eID it becomes apparent that pseudonymisation, at least under the working definition of GDPR Article 4(5), can only be achieved in the cases where user authentication is performed through attributes that do not contain identifying information. An attribute is *"any property that describes some aspect about a natural person."*[600] Some attributes are identifying (e.g. the attribute of a person's name), while others are not (e.g. an attribute of a person's age).[601] An authentication is accompanied by a set of attributes, enough to securely prove that a person has authorised access to a resource in the system. In certain schemes, the value of some attributes can be substituted by a pseudonym that performs the same function, i.e. a pseudonym can replace an identifier traditionally used to uniquely distinguish users of the system. However, if the pseudonym is accompanied by identifying attributes in the same dataset, this dataset cannot be considered as pseudonymised for the purposes of the GDPR. A pseudonymised dataset, thus, would only contain a combination of pseudonyms and non-identifying attributes, such as age or address (if the address is sufficiently expanded to a street or neighbourhood rather than a particular house, see table 7.1).

From a technological perspective, eID schemes have the capability to construct pseudonymised datasets through the process of 'selective disclosure'. Selective disclosure protocols allow eID schemes to select a subset of the attributes of the person and transmit only those absolutely necessary for the needs of each service,[602] i.e. if a service only needs to know whether a user is above a certain age, the scheme can reply with only a

[598] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, rec 28.

[599] ibid rec 26.

[600] George Danezis and others, *Privacy and Data Protection by Design – from policy to engineering* (ENISA report, 2014) DOI: 10.2824/38623 25; by Modinis definition: *"a distinct, measurable, physical or abstract named property belonging to an entity"* Modinis IDM Study Team (ed), *Common Terminological Framework for Interoperable Electronic Identity Management* (techspace rep, 2.01, Europäische Gemeinschaft - eGovernment Unit 2005) ⟨https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf⟩ accessed 17 January 2020 (archived at ⟨https://tinyurl.com/yxyt942w⟩) para 4.4.

[601] Danezis and others (n 600) 25: *"The following items are examples of attributes: your name, age, date of birth, colour of hair, diplomas, grades, subscriptions, event tickets, to name but a few. Some attributes are static (like date of birth), others are dynamic (like a subscription to a newspaper). Some are identifying (your name) while others are not (your age, if the anonymity set is large enough)."*

[602] Andreas Pfitzmann and Marit Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology* (v0.33, 2010) ⟨https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.doc⟩ accessed 12 June 2015 (archived at ⟨https://tinyurl.com/ycshm2ey⟩) fn 2 and accompanying text.

	Unique ID	Name	DOB	Address	Previous address
1.	E2N14JB70	Joe Black	10/10/1970	5 Victoria Rd, London, E2N14, UK	45 University Rd, Reading, RG5E3, UK
2.	HMRC75	User 75	10/10/1970	5 Victoria Rd, London, E2N14, UK	—
3.	HMRC75	User 75	1970	E2 UK	—

GDPR characterisation: 1. Identifying 2. Identifiable 3. Pseudonymised

Table 7.1: Pseudonymised eID datasets under the GDPR

pseudonym for the particular user and a Yes/No answer.[603] Selective disclosure would thus appear to be a means to effectuate pseudonymisation (and data minimisation). Whether the data could be considered as pseudonymised would depend upon the practices of recipients of the eID means, and in particular profiling practices.

The strict formulation of pseudonymisation by the GDPR presents challenges for the operation of eID schemes. This is not to say that pseudonymisation as formulated is unattainable; as discussed above it is technically possible to construct pseudonymised eID datasets using selective disclosure. It is challenging, rather, because of the way eIDAS has conceived pseudonymisation and data minimisation within the Interoperability Framework.

7.3 Pseudonymisation under the Interoperability Framework

As aforementioned the Interoperability Framework defines a set of common high-level rules or principles for identification and authentication:

- a set of LoAs that should be mapped against the supported assurance levels of the national schemes;[604]
- a set of minimum technical requirements;[605]
- a set of minimum *"person identification data"*;[606]
- procedural and dispute resolution rules;[607]
- compliance with data protection rules;[608]
- facilitation of privacy by design.[609]

[603] The given example actually goes a bit beyond simple selective disclosure, as aside from transmitting only selected attributes it also performs a calculation: it derives the present age from a date of birth and compares it with a given value.

[604] eIDAS (n 565) arts 12(4)(b), 6(1)(b).

[605] ibid arts 12(4)(a), 12(4)(c).

[606] ibid art 12(4)(d).

[607] ibid arts 12(4)(e), 12(4)(f), 12(4)(g).

[608] ibid arts 12(3)(d), 5(1).

[609] ibid art 12(3)(c).

The common rules, which were explained in detail in sections 3.2.1, 3.2.2 and 3.4.2, are complemented by the respective implementing acts that further refine the high-level requirements. The combined set of principles, although aiming to be technology-neutral, contains in practice certain technological assumptions.

One of these technological assumptions has to do with the existence of the Minimum Dataset.[610] The Minimum Dataset is defined in IR 2015/1501. It shall contain such attributes that will *"uniquely represe[nt] a natural or legal person"*.[611] Where a legal person performs authentication, the authentication will also be accompanied by a Minimum Dataset of the natural person that represents the legal person, which *"shall contain the combination of the attributes [...] for natural persons and legal persons"*.[612] The Minimum Dataset was seen as a necessary compromise: online public services would typically require this amount of information to be able to uniquely distinguish a person.[613]

The attributes are specified in the ANNEX of IR 2015/1501. For a natural person, a mandatory[614] and an optional set[615] are defined: The *"current family name(s)"*, *"current first name(s)"*, *"date of birth"* and *"a unique identifier [...] which is as persistent as possible in time"* are mandatory. Optionally, the set may also contain the *"first name(s) and family name(s) at birth"*, the *"place of birth"*, the *"current address"* and the *"gender"*. The Minimum Dataset is expected in all authentications *"when used in a cross-border context."*[616]

The presence of the Minimum Dataset actively limits the level of pseudonymisation that can be achieved within the Interoperability Framework. The limiting factors are, on one hand, the stipulation of a unique identifier *"as persistent as possible"* and, on the other, the existence of the Minimum Dataset itself (at least its mandatory part). Unique identifiers have been associated with privacy risks, as their use across multiple services can enable future tracking and profiling.[617] And, although the identifier needs to only be as persistent *"as possible"*, neither eIDAS nor the implementing acts specify the permissible window of time after which identifiers are allowed to change. Besides, the persistence creates tensions with the effective use of pseudonyms.

[610] Other technological assumptions include, for example, the methods of deployment of the eIDAS nodes, as explained in section 3.2.2.

[611] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1, art 11(1).

[612] ibid art 11(2).

[613] European Commission, *"IMPACT ASSESSMENT: Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market "* (Commission staff working paper) SWD(2012) 135 final, 33.

[614] Impl Reg 2015/1501 (n 611) ANNEX 1: *"...shall contain all of the following mandatory attributes..."*

[615] ibid ANNEX 1: *"...may contain one or more of the following attributes..."*

[616] ibid arts 11(1), 11(2).

[617] Danezis and others (n 600) 27.

In privacy-minded schemes, unique identifiers could be replaced by randomly constructed pseudonyms. This could be a valid option even for cross-border transactions, since the format of the unique identifier is a decision of the sending Member State. In fact, eIDAS goes as far as to include a non-prohibition clause for the use of pseudonyms in eID in its general provisions.[618] However, extensive use of a persistent pseudonym will in practice transform the pseudonym to a *de facto* unique identifier.[619] Note that this limitation is not by design. It is rather a *functionality creep*,[620] a limitation posed by the implementation of the Interoperability Framework.

Further, as explained in section 7.2, the mere existence of a pseudonym in the dataset is not enough to render that dataset pseudonymised if the remaining attributes contain identifying information. The Minimum Dataset *must* contain all of the mandatory attributes. And, even though the inclusion of any of the optional attributes is at the discretion of the Member State, is such attributes are included there is no mechanism provided to selective disclose them when needed. As a result, the Minimum Dataset cannot undergo pseudonymisation since the mandatory attributes will always be identifying.

It seems, therefore, that full selective disclosure cannot be an option for cross-border exchanges. At least in so far as attribute-based selective disclosure is not possible for the Minimum Dataset.[621] It is interesting to note that in the preparatory reports leading up to the proposal for eIDAS, one of the necessary characteristics of the proposed *"pan-European eAuthentication system"* was that *"users would no longer be pushed to 'over-identify' themselves in order to gain access to a certain service. Only specific attributes related to the transaction should be corroborated."*[622]

Such a choice could be explained by the necessity to accommodate all available national architectures, since implementation varies from schemes with central governmental databases that use a Central Residents Register number as a unique identifier,like Estonia's,[623] to schemes employing a varying unique identifier (thus essentially a pseudonym) like

[618] eIDAS (n 565) art 5(2): *"the use of pseudonyms in electronic transactions shall not be prohibited."*

[619] See for example *Michigan Department of State v United States* 166 F Supp 2d 1228 (US 2001) on such *de facto* transformation of the US Social Security Number to a national unique identifier.

[620] Niels Vandezande, *"Identification numbers as pseudonyms in the EU public sector"* (2011) 2(2) European Journal of Law and Technology, 1 ⟨http://ejlt.org/article/view/65/142⟩ , 5.

[621] See, for example, Harald Zwingelberg and Jan Schallaböck, *H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective* (v1.0, ABC4Trust 2013) ⟨https://abc4trust.eu/download/ABC4Trust-H2.4_Privacy_Perspective_on_the_eIDAS_regulation.pdf⟩ accessed 12 May 2016 (archived at ⟨http://archive.fo/1kPEw⟩) 6–8 where the authors explain how pseudonyms and selective disclosure can enhance scheme privacy.

[622] Citing the following example: *"to the question: 'Is the user older than 18?' the system would provide only 'yes/no' answer, and not the user's whole birth date"*: DLA Piper and others, *Proposal for a European IAS policy framework: Feasibility Study on an electronicidentification, authentication andsignature policy (IAS)* (Study carried out for the European Commission, D3, version 2b (final), 2013) ⟨https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2794⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ycg95yvm⟩) 157.

[623] Tarvi Martens, *"Electronic identity management in Estonia between market and state governance"* (2010) 3(1) Identity in the Information Society 213 DOI: 10.1007/s12394-010-0044-0, 214–220.

Austria[624] and schemes designed specifically to disallow the existence of such unique identifiers, like Germany's nPA.[625] Note that National Unique Identifiers, in the form of Austria's Central Residents Register, are not the only identifiers of national-wide application. Unique identifiers of eID schemes could be regarded as *de facto* national unique identifiers if they gain wide use.[626] Identifiers that are extensively reused in multiple cases or multiple sectors (*"functionality creep"*)[627] are in practice transformed to what Article 87 of the GDPR terms an *"identifier of general use"*.[628] Consequently, a unique number that links a citizen's eID with public-sector records about their activity could potentially be regarded as a *de facto* National Unique Identifier.

The use of pseudonyms was not the norm at the time of the adoption of eIDAS, although pseudonyms have lately been integrated into the design of Member States' national schemes. The way national eID implementations are approaching pseudonymisation as of recently is further explored in chapter 8. Such an evolution seems compatible with Article 87 of the GDPR which appears to acknowledge that Member States are free to choose any identifier in place of a national identification number.[629] Note, however, that for national identification numbers or *"any other identifier of general application"*, Article 87 permits processing only *"under appropriate safeguards for the rights and freedoms of the data subject"*. Article 87, therefore, directly references data protection by design and eID schemes that use identifiers of general application should only do so under appropriate technical and organisational safeguards.

As a result, one could try to argue that since the GDPR shall complement eIDAS for all types of services (through Article 5(1) eIDAS), Article 25 of the GDPR would require national eID schemes to embed full selective disclosure functionalities.[630] To argue the contrary one would need to demonstrate that not promoting full selective disclosure can be justified in particular by taking into account the cost of implementation as well as the nature, scope, context and purposes of processing. Yet, as aforementioned justification of the measures cannot be based solely on economic considerations.[631] Further, some national schemes of Member States have opted for selective disclosure[632] and a few

[624] Thomas Rössler, *"Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government"* (2008) 24(5) Computer Law & Security Review 447 DOI: http://dx.doi.org/10.1016/j.clsr.2008.07.006, 448–451.

[625] Andreas Poller and others, *"Electronic Identity Cards for User Authentication - Promise and Practice"* (2012) 10(1) IEEE Security & Privacy 46 DOI: 10.1109/msp.2011.148, 46–47.

[626] Such is the case, for example, in the US where the Social Security Number is being used across finance, employment and governmental agencies. See for example *Michigan Department of State v United States* (n 619) 1232–1233 on its use when applying for a driving license.

[627] Vandezande (n 620) 5.

[628] GDPR (n 598) art 87.

[629] ibid art 87: *"Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application"*.

[630] ibid art 25: *"implement appropriate technical and organisational measures, such as pseudonymisation"*.

[631] See balancing test of figure 4.1.

[632] See section 8.3 and Poller and others (n 625) 54: *"The user is presented with the authorization certificate and has the option to deselect data fields from the service authorization."*

solutions have already been discussed in the literature.[633] Hence, such an argument appears unlikely to persuade.

Mutatis mutandis the same should apply in the case of electronic certificates when used for eID. Certain national schemes, e.g. the scheme of Belgium,[634] retrieve the attributes that form the Minimum Dataset from a stored electronic certificate. Potentially, certain certificates could be rich in personal data. The distribution of such certificates internally, within one Member State, but also across borders, between Member States, would then raise serious data protection compliance issues, as the sharing of personal data requires both security measures and data-protection-by-design measures in place.[635] On this point, it is striking to note that recent literature in the field of anonymisation attempting to map security and data protection by design measures to a spectrum of data sharing scenarios takes the view that the sharing to the public of personal data is risky as long as de-identification and generalisation techniques such as k-anonymity are not implemented.[636]

It should also be noted that certificates do not pose risks only when used as eID means: in the simple scenario where a (qualified) certificate is being used to electronically sign an email, the email recipient has the ability to view and store the certificate in order to verify the authenticity of the e-signature. Besides, digital certificates are also stored in certificate repositories.[637]

Yet, eIDAS does regulate the content of certificates (in particular in its annexes such as Annex I on requirements for qualified certificate for electronic signatures) but simply allows the use of pseudonyms instead of real names without making it mandatory, as per

[633] See for example Stefan Brands, *"Rethinking Public Key Infrastructures and Digital Certificates"* (The MIT Press 2000) 91–130; Gergely Alpár and Jaap-Henk Hoepman, *"A Secure Channel for Attribute-based Credentials: [Short Paper]"* (Berlin, Germany, ACM Workshop on Digital Identity Management, 8 November 2013, DIM '13, ACM 2013) DOI: 10.1145/2517881.2517884 14–17.

[634] Jan van Arkel, Marc Lange, and Henry Ryan, *Towards an electronic ID for the European Citizen, a strategic vision: CEN/ISSS Workshop eAuthentication* (0.17, 2004) ⟨https://danishbiometrics.files.wordpress.com/2009/08/doc.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/rrykxr8⟩) 17.

[635] See e.g. the Belgium case where in principle restrictions are in place: the use of the *"national identification number"* is restricted to pre-defined data processing operations by entities pre-authorised by the Belgian Privacy Commission and cross-linking of the number across uses is highly regulated. See Jos Dumortier and Niels Vandezande, *"Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market"* [2012] ICRI Research Paper 9 ⟨http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152583⟩ accessed 25 December 2016 , fn 5 and relatex text.

[636] Orit Levin and Javier Salido, *The Two Dimensions of Data Privacy Measures* (Research Paper, Microsoft: Corporate, External and Legal Affairs 2016) ⟨https://fpf.org/wp-content/uploads/2016/11/The-Two-Dimensions-of-Data-Privacy-Measures.pdf⟩ accessed 28 November 2016 (archived at ⟨http://archive.fo/SfBCD⟩) 1–2.

[637] See the Certificate Status Tool, which is described as being *"designed to provide certificate status information based on manually defined trust anchors as well as the EU Trusted Lists of Certification Service Providers (TSL)"*: *"Certificate Status Application"* (*Secure Information Technology Center – Austria*, 2019) ⟨https://demo.a-sit.at/certificate-status-application/⟩ accessed 16 June 2019.

Article 5(2). As some Member States[638] have opted for pseudonyms there is a strong argument that certificates should only contain pseudonyms. And, although the principle of data protection by design only applies to data controllers, service providers that issue electronic certificates should be characterised as data controllers.[639]

At the very least, it would be good practice for service providers to base decisions about their system architecture on data protection by design assessments, in particular when these decisions are likely to affect a large number of data subjects at regional, national or even supranational level. And processors, though not strictly captured by the obligation, should assist data controllers in that respect.

Constraining the levels of selective disclosure and pseudonymisation is surprising. The Interoperability Framework could impact, in some cases negatively, the level of data protection by design guaranteed by national eID schemes. Article 8 and the three LoAs do not guarantee that data protection levels set at the national level will not be affected. But an impact would arguably be contrary to eIDAS Article 12(3)(c) and Article 12(3)(d) which promote privacy by design and data protection. Besides, an impact would likely trigger consequences in terms of liability for data controllers (as GDPR Article 82 should be combined with eIDAS Article 11), i.e. for Identity Providers, Service Providers that issue electronic certificates and the entities operating the national eID schemes. A low(er) level of unlinkability, and hence of data protection by design, can only be justified if compared to the state of the art and the cost of implementation.[640]

7.4 Conclusion

Under the GDPR, pseudonymised datasets are only the datasets where no identifying information accompany the pseudonyms. In the field of eID, this can only be achieved when none of the attributes contained within a dataset can, even if combined with other information, identify an individual. Hence, in practice pseudonymised eID datasets will only be datasets that contain non-identifying attributes, such as age or city of residence.

As a result, effective pseudonymisation in eID schemes can only be achieved when coupled with selective disclosure. Selective disclosure will permit for identifying information

[638] See e.g. Vandezande (n 620) s 3.2 about ssPIN and digital signatures in Austria; Federal Office for Information Security [BSI], *"TR-03110 eIDAS Token Specification"* (*Federal Office for Information Security*, 5 January 2016) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile~%5C&~v=1⟩ accessed 12 January 2016 s. 2.2.4.

[639] As is the case, for example, in the UK e-Science PKI: Science and Technology Facilities Council, *UK e-Science Certification Authority Certificate Policy* (2.0, 2015) 43 which specifies that *"[t]he data controller is the [Certification Authority] Manager"* and *"[t]he data processor is any [Registration Authority] Manager or Operator"*.

[640] The other contextual factors of GDPR (n 598) art 25(1), the nature and scope of processing and the risks to the rights and freedoms of the data subjects have already been examined through the threshold analysis.

to be discarded so that only pseudonymised attributes remain. However, the current specification of the Interoperability Framework do not permit selective disclosure: the Minimum Dataset set up by eIDAS contains a strict set of mandatory attributes that are always present. And even though in principle pseudonyms are allowed under Article 5(2), they are rendered as *de facto* unique identifiers because of the absence of selective disclosure.

Hence this practice negates any pseudonymisation functionality, lowering the level of unlinkability supported. This is problematic if a participating Member State relies on a high level of unlinkability, as participating in eIDAS will have the effect of lowering the level of data protection by design guaranteed by its national eID scheme.

To understand whether this is a justified trade-off, one needs to assess it against the other contextual factors of Article 25: the state-of-the-art and the cost of implementation. The next section will look at three exemplary implementations of eID schemes, analysing their architecture, their privacy features and the controls implemented to serve unlinkability. This will enable the characterisation of the state of the art in the field of eID.

Chapter 8

National implementations of eID

Taking into account the state of the art...

— GDPR Art 25

producers of the products, services and applications should[...], with due regard to the state of the art, [...]make sure that controllers and processors are able to fulfil their data protection obligations.

— GDPR Rec 78

8.1 Introduction

As explained in section 7.3 the Interoperability Framework supports a level of unlinkability through mainly its prescription about data minimisation for cross-border transactions. However, it was shown in chapter 6 that unlinkability is a key goal for data protection by design. After all, if eID is considered as likely to result in high-risks,[641] a high level of unlinkability with appropriate safeguards would be expected.

This chapter examines the state of the art in terms of data protection by design, and specifically in terms of unlinkability, in the field of national eID schemes. The state of the art is essential, as a contextual factor to determine whether the safeguards offered by the Interoperability Framework address unlinkability adequately.

Three national schemes are examined: the Austrian 'Citizen Card', the German 'new Personal ID Card' and the UK 'Gov.UK Verify'. The goal is to explore how national eID schemes have embedded privacy and data protection requirements, in order to determine the potential effects of GDPR Article 25. The three national schemes have been selected on the basis of two considerations: First, they all represent distinct architectural models, deploying eID federation through a mix of public and private sector parties. Second, they all have been built with due consideration to privacy and data protection and therefore

[641] As is the opinion of the UK ICO, see n 440.

rely upon a series of privacy and data protection claims. Although all three schemes essentially use a federated model, their architecture differs significantly: Germany has deployed a decentralised system, whereas Austria and the UK use federation with some centralised components. At the same time, Germany relies on the use of a hardware token as the eID means, while the UK uses a software token and Austria uses a combination of both.

Section 8.2 presents the natioal eID scheme of Austria, explaining the main actors and data flows in section 8.2.1. The national eID scheme of Germany is presented in section 8.3, with the main actors and data flows explained in section 8.3.1. UK's national eID scheme is presented in section 8.4, with its actors and data flows in section 8.4.1. Based on the analysis that was presented in the previous chapters, the impact that the participation in the Interoperability Framework will have for each national eID scheme is discussed in section 8.5. Note that the material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness.*[642] Part of the material was published under *"Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation"*; *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"*; *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[643]

8.2 The Austrian Citizen Card

The Austrian Citizen Card (ACC) is defined under the Austrian E-Government Act 2004.[645] It is designed around the existence of a Central Residents Register (CRR), but deployed following a federated architectural model. The CRR serves as a national

[642] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[643] Niko Tsakalakis, Kieron O'Hara, and Sophie Stalla-Bourdillon, *"Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation"* (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), 21 May 2016, Hannover, Germany, 2016) DOI: 10.1145/2908131.2908152; Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (2017) 3(3) The Journal of Web Science 32 DOI: 10.1561/106.00000010; Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

[644] Stefan Strauß and Georg Aichholzer, *"National Electronic Identity Management: The Challenge of a Citizen-centric Approach Beyond Technical Design"* (2010) 3(1) International Journal on Advances in Intelligent Systems 12 , 17.

[645] Federal Act on Provisions Facilitating Electronic Communications with Public Bodies 2004, BGBl I Nr. 10/2004, amended by BGBl I Nr. 7/2008 and BGBl I Nr. 59/2008 [Austrian Federal Law] (Austrian E-Government Act 2004).

database where each Austrian resident is assigned a CRR number. CRR numbers are strictly regulated by Austrian law which makes their use *"undesirable"* due to privacy reasons.[646] Instead the ACC binds a person's eID data on a specially derived unique identifier, called the source Personal Identification Number (sPIN). The sPIN is an algorithmically encrypted value of the CRR number.[647] sPINs are only created by the sPIN Register Authority, under the Austrian Data Protection Commissioner, and are only stored in a person's eID card (figure 8.1).[648] Citizens can identify themselves against Service Providers by presenting the card and entering a password. The card carries a qualified electronic certificate, used to create electronic signatures. The card authorises the release of a special XML data structure (named *"Identity-Link"*), signed by the sPIN. The Identity-Link includes the citizen's sourcePIN, first name, last name, date of birth, and a qualified certificate for creating digital signatures.[649] The Identity-Link is

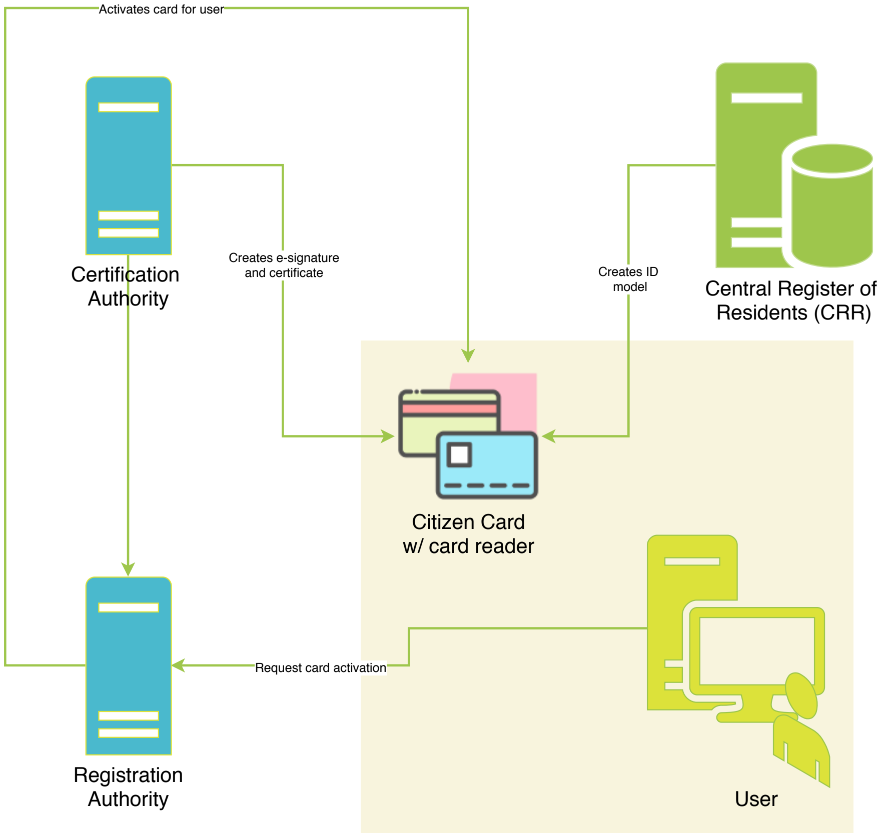


FIGURE 8.1: ACC eID means issuance[644]

[646] Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991) 1992, BGBl. I Nr. 9/1992, [Austrian Federal Law] (MeldeG 1991) s 16a.

[647] Thomas Rössler, *"Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government"* (2008) 24(5) Computer Law & Security Review 447 DOI: http://dx.doi.org/10.1016/j.clsr.2008.07.006, 448.

[648] Aside from this client-based model, the Austrian system also supports a server-based model which allows for eID through mobile devices.

[649] Daniel Slamanig, Klaus Stranacher, and Bernd Zwattendorfer, *"User-centric Identity As a Service-architecture for eIDs with Selective Attribute Disclosure"* (SACMAT '14, ACM 2014) DOI: 10.1145/2613087.2613093 158.

then verified against the citizen's (qualified) electronic signature's public key. If the two match, *"it can be strongly assumed that the person who possesses the signature creation device (i.e. the Citizen Card) and knows the secret code required to release signature creation is the person described in the Identity-Link."*[650] Although the assumption is the use of a card, the scheme has been designed to be technology neutral, with current implementations including public and private smartcard tokens (for example, the health insurance card) or mobile tokens.[651] After successful verification of the sPIN, the user is authenticated against the Service Provider by sending a data structure that includes personal attributes (e.g. name, age) and a special unique identifier specific to the Service Provider and the user (called an sector-specific Personal Identification Number (ssPIN)).[652] Communication between the parties uses the SAML protocol.

8.2.1 ACC Actors and Data Flows

The main actors in an ACC authentication process are:

(1) The User, equipped with either (a) a **smartcard eID** or (b) a **mobile eID** token.

(2) A **middleware**, interfacing with the user's smartcard or mobile eID token. Smartcard eID tokens interface with the user through software running in the user's computer. Mobile tokens use a mobile eID Service Provider's interface at the user's phone.[653]

(3) The **Service Provider**, which is either a public or private sector body, belonging to one of the pre-defined sectors of state activity. The Service Provider operates a module (MOA-ID) that interfaces with the citizen's eID token through the middleware of item (2).

(4) The Austrian Data Protection Commissioner, and its **sPIN Register Authority** sub-department, in charge of issuance of the base sPIN in the smartcard or mobile token. The sPIN is derived from the Central Residents' Register (CRR).

From the above, item (4) is relevant only at the time of the issuance of the eID means.

The ACC stores a citizen's attributes (including a unique identifier, name and date of birth) within the Identity-Link structure of the citizen card (or mobile eID means).[654] To avoid the privacy threats of persistent unique identifiers, who could potentially lead to data linkage across different domains, processing of a persistent unique identifier (like

[650] Rössler (n 647) 450.

[651] Juraj Somorovsky and Vladislav Mladenov, *D2.2 Overview of eID Services* (FutureTrust Consortium, v 1.0, 2017) 10.

[652] See section 8.2.1.

[653] Somorovsky and Mladenov (n 651) 11.

[654] Slamanig, Stranacher, and Zwattendorfer (n 649) 154.

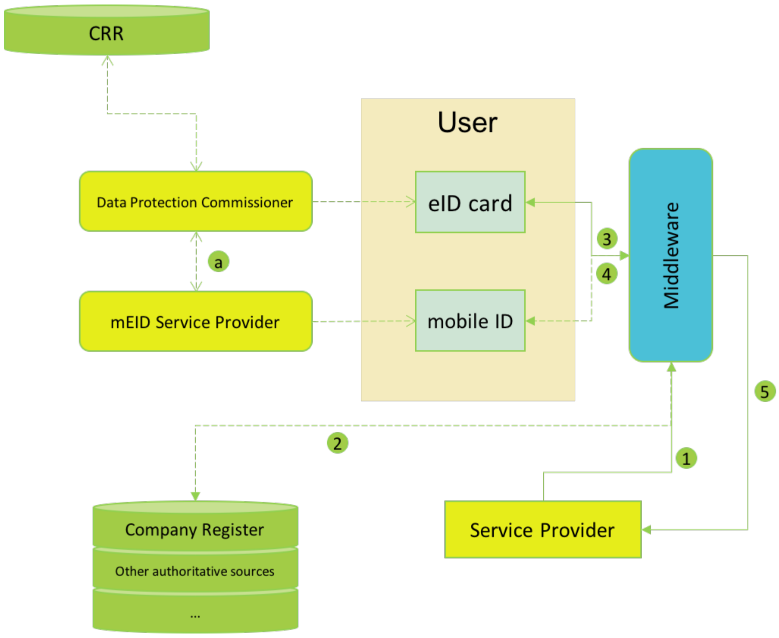


FIGURE 8.2: ACC data flow

the sPIN) is prohibited. Instead the scheme creates a unique identifier per domain of application (the ssPIN). The ssPIN is constructed by hashing a user's sPIN along with the identifier of the domain it will be used in, i.e. a pairwise identifier.[655]

In Austria all governmental applications are divided into different sectors, or domains, by law. There are currently 35 different sectors, and they can be further segmented if applicable.[656] Each sector is assigned a different alphanumeric code.[657] For each of these sectors an ssPIN is created by combining the hashed value of the user's sPIN with the hashed value of the sector's alphanumeric code. Each ssPIN is different and because of the hashed values it is impossible to reverse engineer the underlying sPIN value.[658] At the moment only 26 from the 35 domains of application are in use; domain-specific identifiers are limited by law to be used only within the domain they were created for. It is also prohibited to persistently store the sPIN outside of the citizen card. Hence the ACC deploys what can be seen as 26 different pseudonyms for each user which accompany the identifying dataset.[659]

[655] Pairwise (pseudonymous) identifiers are identifiers constructed for the unique pair of sender and recipient (i.e. the citizen and the specific Service Provider). See OASIS, *SAML V2.0 Subject Identifier Attributes Profile* (Committee Specification 01, Version 1.0, 2019) ⟨http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html⟩ accessed 17 February 2020 (archived at ⟨http://archive.is/ri9U6⟩) s 3.4.

[656] Austrian E-Government Act 2004, s 3(1).

[657] E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV) 2004, BGBl II Nr. 289/2004, [Ordinance of the Federal Chancellor, with which the state activities are defined for the purpose of the identification in e-government communications] (Austrian Administrative Act 2004 (E-Gov-BerAbgrV)) s 6.

[658] Rössler (n 647) 449.

[659] Georg Aichholzer and Stefan Strauß, *"The Austrian case: multi-card concept and the relationship between citizen ID and social security cards"* (2010) 3(1) Identity in the Information Society 65 DOI: 10.1007/s12394-010-0048-9, 18.

Accordingly, pseudonymisation is provided by the scheme in the form of ssPINs (with 26 possible combinations of user sPIN ⟷ Service Provider sPIN for the 26 sectors they are currently available).[660] On the other hand, the presence of an accompanying dataset of identifiers (name, date of birth) does not guarantee that selective disclosure is being used, or to what extend. In fact, some authors have commented on the lack of transparency on how the identifiers are being deployed in the scheme raising concerns not only as regards the users' amount of effective control but also the risk of data linkage despite the deployment of ssPINs.[661] Austria has not yet publicly announced any plans to notify ACC. In light partly of eIDAS, and discussions about solutions for better selective disclosure and anonymity,[662] Austria is currently undergoing a redesigning of its scheme.[663]

The authentication process starts with the user requesting to access a service that requires authentication.

(1) The Service Provider launches a SAML authentication request directed at the user's middleware (computer software or mobile device interface).

(2) The middleware receives the request under a session handle and validates the Service Provider's identity.

(3) The user selects either their smartcard or mobile eID tokens for authentication. The middleware then derives the ssPIN by hashing the eID means' sPIN and the Service Provider's sector identifier.

(4) An authentication prompt is presented to the user, containing the Service Provider requesting the authentication, its sector identifier and the attributes requested.

(5) After user consent (through a qualified electronic signature), the authentication block and electronic signature is validated by the Service Provider and the SAML response is returned to allow access to the service.

8.3 The German nPA

The German 'neuer Personalausweiss (nPA)' makes Germany's national ID card its core component. The card is equipped with a RFID chip, where an electronic attestation

[660] Aichholzer and Strauß (n 659) 73.

[661] ibid 19.

[662] See eg Slamanig, Stranacher, and Zwattendorfer (n 649); Bernd Zwattendorfer and Daniel Slamanig, *"On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud"* in Lech J Janczewski, Henry B Wolfe, and Sujeet Shenoi (eds), *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings* (Springer Berlin Heidelberg 2013) DOI: 10.1007/978-3-642-39218-4_23.

[663] The redesigned scheme is introducing a central hub, non-transmission of the sPIN outside of the sPIN Register Authority, end-to-end encryption and a 'history' function so users can see where their eID means has been deployed. See Austrian interview, lines 90–136, s. 11 Appendix I: Interview transcripts.

of the identifying information is stored. The included attributes are the forename and surname, the current address with the postcode and the municipality ID, the date of birth, the nationality, the place of birth, the card's expiry date, and, optionally, the fingerprints.[664] The card improved on the previous username/password authentication by enabling two-factor authentication to be used in the scheme. In order to authenticate, users are required to use the eID card and a personal PIN. Users authenticate directly to Service Providers, via Single Sign-on (SSO) and SAML or Simple Object Access Protocol (SOAP). The scheme offers three-way end-to-end cryptography between the user and the Service Provider; a card reader at the possession of the user validates the card, then the reader validates the identity of the Service Provider and finally the Service Provider authenticates the user through electronic certificates.[665] The implementation does not depend on an Identity Provider. Although strictly speaking there is a central governmental Identity Provider, operated under the Federal Office for Information Security (BSI), its role is to authenticate the identity of the Service Providers, not the users. The scheme, thus, can be characterised as totally user-centric, with the user being in the sole control of their eID means and its uses. All identifiers are stored on the card at the moment of creation. The cards are produced 'offline' in the Federal printing facilities; after production all data are required by law to be erased from the facilities and the government has no technical means of tracking or monitoring individual card usage. The cards only operate in offline mode, meaning all identifiers are validated locally without transmission over a network. Online communication with the Service Provider happens through middleware software at the possession of the user.[666]

The basic premise behind the scheme's design is that an identifying set of attributes[667] has greater value after having been validated as trustworthy from an official source (i.e. the national scheme) and, therefore, deserves greater protection (than other sets of identifying information). To safeguard the card's identifiers the scheme shall minimise transmission of identifiers (data minimisation), allow for creation of multiple electronic identities (pseudonymisation) and each electronic identity shall be able to combine any

[664] Federal Office for Information Security [BSI], *Architecture electronic Identity Card and electronic Resident Permit* (Technical Guideline, TR-03127 v1.13, 2011) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf⟩ accessed 23 May 2016 (archived at ⟨http://archive.fo/IoGbj⟩) 6. Currently no eID application in Germany is designed to use fingerprint authentication. Additionally, serial numbers for the card and the chip and a biometric photo similar to ePassports are available to elevated governmental terminals: Andreas Poller and others, *"Electronic Identity Cards for User Authentication - Promise and Practice"* (2012) 10(1) IEEE Security & Privacy 46 DOI: 10.1109/msp.2011.148, 4–5.

[665] Federal Office for Information Security [BSI], *"The German eID"* (*Federal Office for Information Security*, 2017) ⟨https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html⟩ accessed 8 March 2017 (archived at ⟨http://archive.fo/gzHLy⟩) 7.

[666] The Government has released a multi-platform free programme, called 'AusweisApp' free of charge. For more see: https://www.ausweisapp.bund.de/ausweisapp2/.

[667] referred to as *"sovereign data set"*; in other literature this dataset is referred to as *"transaction identity"*. See eg Clare Sullivan, *"Digital identity, an emergent legal concept: the role and legal nature of digital identity in commercial transactions"* (University of Adelaide Press 2011) 43–49.

number of identifiers according to use case (selective disclosure).[668] The scheme, by design, prohibits Service Providers to store authenticated data and authentication is dependent upon Service Provider-specific pseudonyms. Notably there is potential for inter-linking of data, if an entity sub-contracts their eID services to another Service Provider. In this case, linking a pseudonym to multiple uses is technically possible, therefore increasing the potential to infer the user associated with the pseudonym. Hence, policy measures complement the technical design – linking of data is forbidden by law.[669]

8.3.1 nPA Actors and Data Flows

There are three main actors in the German nPA during an authentication process:

(1) The **user**, equipped with their national eID card and a suitable terminal. There are several solutions for terminals, ranging from traditional card readers connected with a personal computer to mobile phones using RFID tags. All of them interface with the 'AusweisApp', a software provided by the BSI (or other BSI approved client software).

(2) The **Service Provider**, operating an eID server that can communicate with the eID card either via SOAP or SAML.[670]

(3) The BVA,[671] which acts as an Identity Provider to validate the identity of the Service Provider through electronic certificates.

Technically speaking, the BVA (item (3)) is not involved directly into the authentication transaction. Instead, it is the body who issues validated electronic certificates to Service Providers so that they can request data from eID meanss (points (a) and (b) in figure 8.3).

[668] Gilad L Rosner, *"Identity management policy and unlinkability: a comparative case study of the US and Germany"* (PhD thesis, University of Nottingham 2014).

[669] German law is rich in privacy-enhancing principles. At the core is the *"right to information self-determination"* which is a German inception. It confers the right to decide when and within what limits information about one's self should be communicated to others: Gerrit Hornung and Christoph Schnabel, *"Data protection in Germany I: The population census decision and the right to informational self-determination"* (2009) 25(1) Computer Law & Security Review 84 DOI: 10.1016/j.clsr.2008.11.002, 85–86. The right stemmed from a decision of the German Constitutional Court: *Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 Oktober 1983* (1983) 65 BVerfGE 1 (in den Verfahren über die Verfassungsbeschwerden [in German]). The Court further prohibited any future creation of a persistent unique identifier, ibid s 1. Additionally public authorities operate under a *"separation of informational powers"* – they are not allowed to collate data, as the state should not operate as a single entity, and all data transfers have to be justified against the principles of 'purpose specification' and 'proportionality': Herbert Burkert, *"Balancing informational power by informational power or Rereading Montesquieu in the internet age"* in Eric Brousseau, Meryem Marzouki, and Cécile Méadel (eds), *Governance, Regulation and Powers on the Internet* (Cambridge University Press 2012) ⟨http://dx.doi.org/10.1017/CBO9781139004145.006⟩ 101–102.

[670] Federal Office for Information Security [BSI], *Technical Guideline TR-03130 eID-Server: Part 1: Functional Specification* (v 2.1.2, 2017) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part1.pdf?__blob=publicationFile&v=3⟩ accessed 27 February 2019 (archived at ⟨http://archive.fo/5Njov⟩) 9–14.

[671] The Federal Office of Administration, a federal authority of the Federal Ministry of the Interior.

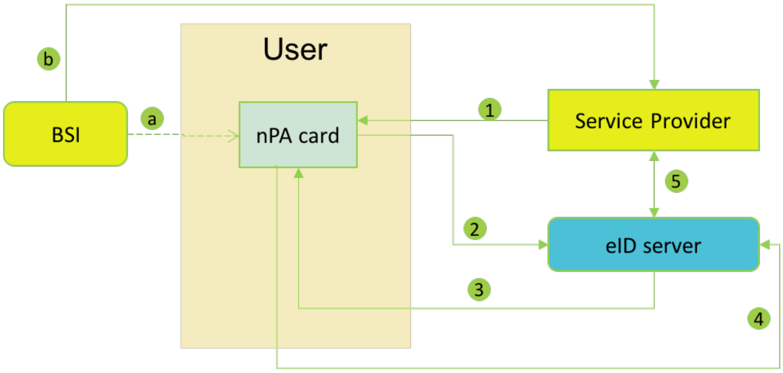


FIGURE 8.3: nPA actors and data flows

The BVA is also operating eID servers that Service Providers can connect to perform authentications, if the Service Providers are not operating their own eID server. A fourth actor can be observed during the first issuance of an eID card: The Bundesdruckerei (Federal Printing Office) is in charge of issuing new cards, on behalf of the Ministry of the Interior; however, it has no further role after printing the card.

When a user is requesting access to an electronic service that requires authentication, the authentication process is as follows (figure 8.3).

(1) A user visits the Service Provider and requests a service. The Service Provider sends an authentication request to the eID card terminal (software and reader, or mobile device).

(2) The terminal validates the authentication request from the Service Provider.

(3) The Service Provider transmits necessary information for the authentication request.

(4) The terminal establishes a secure connection and transmits an authentication block.

(5) The Service Provider fetches the result of the authentication from the eID server.

The scheme allows users to select from a list of potential identifiers before transmission (data minimisation). De-selected fields do not get disclosed. There is no minimum dataset a user has to send over, but deselecting fields could potentially prevent the successful completion of the transaction. Nevertheless, this risk is at the discretion of the user.

The scheme can also perform special functions, i.e. the use of pseudonyms and calculations. For each pair of eID card ⟷ Service Provider the card constructs a specific pseudonym which acts as a unique identifier (similar to ACC's ssPIN) for this specific relationship of user ⟷ Service Provider by combining a cryptographic key stored at the card with one held by the Service Provider. As a result, pseudonyms differ across uses making it impossible to link a user's activities to each other.[672] Additionally, the card is able to

[672] Federal Office for Information Security [BSI], *Architecture electronic Identity Card and electronic Resident Permit* (n 664) 22.

perform calculations to authenticate users in cases where disclosure is not necessary. For example, if access to an electronic service needs prior satisfaction of a legal age claim (i.e. whether the user is an adult), the scheme is able to calculate the user's age based on the date of birth and disclose a Yes/No answer to the claim. Similarly, to a claim of whether a user resides in a certain geographic area (i.e. when a service is available to a certain catchment area), the scheme examines the municipality ID and provides a Yes/No answer to the location claim.[673]

Germany was the first country to pre-notify nPA under Article 9 of eIDAS.[674] After review,[675] the nPA was notified as supporting eIDAS' LoA 'High' (table 8.3), and the notification was published in the Official Journal on 26 September 2017.[676] The BSI has published the conformity reports, detailing how the nPA will operate in conformity with the Interoperability Framework.[677] The conformity specifications determine, among others, how the nPA will satisfy the Minimum Dataset of eIDAS. In particular, it appears that, because of the lack of a unique identifier in the nPA, the *"uniqueness identifier"* of the Minimum Dataset will be substituted by a pseudonym. However, because the pseudonyms created by the nPA are designed to be card-specific or application-specific, the peer-review committee notes that *"the unique identifier provided by the German eID scheme is **not lifelong-persistent**"* [emphasis in the original].[678] As a compromise, BSI decided that for authentications in the Interoperability Framework, the nPA will produce pseudonyms that will remain static for each receiving Member State (table 8.1).

[673] Federal Office for Information Security [BSI], *Architecture electronic Identity Card and electronic Resident Permit* (n 664) 22–23.

[674] Federal Office for Information Security [BSI], *"eIDAS Notification of the German eID"* (*Federal Office for Information Security*, 20 February 2017) ⟨https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html⟩ accessed 27 February 2017.

[675] For a full list of pre-notified and notified national schemes, see table A.1.

[676] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2017] OJ C319/3.

[677] Federal Office for Information Security [BSI], *German eID based on Extended Access Control v2: Overview of the German eID system* (v1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_01_Whitepaper_final.pdf?version=1&modificationDate=1499172188962&api=v2⟩ accessed 22 February 2017 (archived at ⟨http://archive.fo/9Io5h⟩); Federal Office for Information Security [BSI], *German eID based on Extended Access Control v2: LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance* (v1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_02_LoA%20Mapping_final.pdf?version=1&modificationDate=1499172189454&api=v2⟩ accessed 21 February 2017 (archived at ⟨http://archive.fo/qeJZE⟩); Federal Office for Information Security [BSI], *German eID based on Extended Access Control v2: Fulfilment of interoperability requirements according to (EU) 2015/1501* (v1.2, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_03_IF%20Mapping_final.pdf?version=1&modificationDate=1499172189873&api=v2⟩ accessed 21 February 2019 (archived at ⟨http://archive.fo/GWzLJ⟩); Federal Office for Information Security [BSI], *German eID based on Extended Access Control v2: Supporting Documentation* (v 1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_04_SuppDoc_final.pdf?version=1&modificationDate=1499172190074&api=v2⟩ (archived at ⟨http://archive.fo/IxFQ3⟩).

[678] Freek van Krevel, *PEER REVIEW REPORT – German eID* (DG Connect, Digital Single Market, eIDAS Cooperation Network, v 1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/Peer%20review%20report%20German%20eID%20-%2016062017.pdf?version=1&modificationDate=1499172190851&api=v2⟩ accessed 23 July 2019 (archived at ⟨http://archive.fo/3I24w⟩) 18.

Each receiving Member State will be receiving the same pseudonym for a particular user, thereby providing the same pseudonym to all Service Providers of that receiving Member State.[679] The question then is how inter-linkage of eID uses between the Service Providers of a Member State could be prevented. Additionally, the requirement for the existence of all mandatory attributes of the Minimum Dataset appears to also impair the nPA's ability of selective disclosure. Even though the citizens are in principle able to deselect attributes, this will result in a failed authentication.[680]

Opt.[a]	**eIDAS MDS**	**German eID**
M	Uniqueness identifier	Pseudonym[b]
M	Current family name(s)	Family name
M	Current first name(s)	First name
M	Date of birth	Date of birth
O	First name(s) and family name(s) at birth	Birth name (if present on the eID card)
O	Place of birth	Place of birth
O	Current Address	Address
O	Gender	—

[a] *M* = Mandatory attribute, *O* = Optional attribute
[b] The pseudonym of the German eID scheme is specific to each eID card and each receiving Member State (for public-sector bodies) or each relying party (for non-public-sector bodies).

Table 8.1: Minimum Data Set provided by the German eID scheme[681]

8.4 The Gov.UK Verify

UK's Gov.UK Verify differs from the previous two schemes in that it was designed around the absence of a national ID or central citizens registry. It was set to replace the existing solution to access UK online public services,[682] as part of the 2013 Government's *"Digital Strategy"*. It was designed by the Government Digital Service (GDS), part of the Cabinet Office and in charge of the scheme, as a username/password token scheme that would be built around a hub-and-spoke federated architectural model. The eID means (the username/password combination) is supplemented by a second factor of authentication in the form of a 'one-time-password', sent through an SMS, letter, email

[679] *"For public sector relying parties of a receiving Member State the same pseudonym is created even if multiple middleware instances are operated."*: ibid 19.

[680] *"While optional data not required for unique identification (e.g. address) may be deselected by the citizen in the authentication process the minimum data set, however, will always be transmitted and authentication would fail if a citizen deselects one of these data fields for the minimum dataset."*ibid 18.

[681] Federal Office for Information Security [BSI], *"The German eID"* (n 665) 15.

[682] The 'Government Gateway' platform, which is still used for several services: http://www.gateway.gov.uk/Help/Help.aspx?content=help_government_services_online.htm.

or hardware token.[683] A *"Privacy Consumer Advisory Group"* consulted the GDS on nine *"Identity Assurance Principles"* the scheme should adhere to.[684] The nine principles form the bare minimum of operational standards, even though they use a high-level principle-based approach that aims to remain technology neutral. Gov.UK Verify is organised according to *"Identity Assurances"*: it offers different levels of certainty about one's identity, according to a risk-based approach about the connection between the user and the claimed identity.[685] Identity Assurance has been characterised as more consumer led in focus, with no need of central databases, extensive data sharing or data consolidation.[686]

A private market of Identity Providers was created for the purposes of Gov.UK Verify, with the aspiration that consumers will be able to choose which entity they trust more to handle their identification. Gov.UK Verify's users are free to create accounts with multiple Identity Providers, effectively managing multiple electronic identities. The premise was the ability of a user to choose a different eID token according to use, if they so wished. Multiple Identity Providers also assist against data aggregation: eID data are split across the different databases of each Identity Provider, mitigating the risk of a single point of failure. The specification does not constrain the Identity Providers and the Service Providers technology-wise, as long as a translation layer exists, specified by the GDS, to allow inter-communication.

8.4.1 Gov.UK Verify Actors and Data Flows

Gov.UK Verify comprises of five key elements:

(1) The **Verify Hub**: a central infrastructure, owned by the Government Digital Service,[687] that mediates all interaction between users, Identity Providers and

[683] Note that there have been concerns about the assurance that some of these methods provide. In response, *"[t]he UK's Government Digital Service has assessed this specific solution and decided to deprecate it, i.e. it will no longer be allowed to be used by IDPs,and it will be phased out by the end of March 2019."* Agency for Public Management and e-Government, *Peer Review Report – United Kingdom's eID Scheme* (eIDAS Coordination Network, DG Connect, v 1.0, 2018) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/68326890/Final%20version%20of%20UK%20Peer%20Review%20Report_24_01_2019.pdf?version=1&modificationDate=1549037555551&api=v2⟩ accessed 28 July 2019 (archived at ⟨http://archive.fo/afbKM⟩) 22.

[684] Privacy and Consumer Advisory Group, *Identity Assurance Principles* (v3.1, 2014) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1___4__.pdf⟩ accessed 26 May 2016 (archived at ⟨https://perma.cc/5K2W-8BVK⟩).

[685] Justified on the premise that not all transactions require the same level of certainty about somebody's identity. Some only require authentication of an attribute (i.e. that a person is above 18 years old to access age-restricted content).

[686] James Crosby, *Challenges and opportunities in identity assurance* (2008) ⟨http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf⟩ accessed 16 August 2015 (archived at ⟨https://perma.cc/D5RV-WM9U⟩) s 4.

[687] *"[T]he Hub is hosted on Amazon's AWS. The UK emphasized that all hosting regions are based within the EU,to ensure that any processing of personal data takes place under European legislation."*: Agency for Public Management and e-Government (n 683) 27.

Services (or Service Providers). The Hub leases eID services from the private Identity Providers. The Hub acts as a broker to exchanges are sealed from the different parties, ensuring that the Identity Provider remains unknown to the Service Provider. The Hub ensures that the required LOA is adhered to and does not collect or store data beyond the current session (stateless operation).[688] Since there is no data collection, the Hub is not considered as a data controller in regard to data protection.[689]

(2) The **Service Provider** (Relying party): Service Providers are the different public services that can request the eID of the user in order to transact with them. At the moment, Service Providers in the Gov.UK Verify federation are solely governmental departments,[690] which are data controllers for data protection purposes.[691]

(3) The **Identity Provider**: Identity Providers are *"[p]rivate sector organisations, paid by the government, to verify that a user is who they say they are and assert verified data that identifies them to a government service."*[692] They verify the user's identity against various authoritative sources, like the HM Passports Office and the Driving Licensing Authority.[693] For data protection purposes the Identity Provider is considered a data controller.[694]

(4) The **Matching Service**: a middleware deployed at the Service Provider level whose purpose is to match the eID data received by the Identity Provider to a local account in the Service Provider's database.

(5) The **Document Checking Service**: a supplementary service used to validate user data against authoritative sources (the HM Passport Office and the UK's and Northern Ireland's Driver and Vehicle Licensing Agencies) at the point of registration (when a user first creates an account). The service however is provided through API calls of the Identity Providers to the respective authoritative sources and is not directly accessed by Gov.UK Verify.[695] The Document Checking Service does not play a part in further identifications/authentication after the initial account creation.

[688] Government Digital Service, *"Technology Overview"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/technology-overview/#technology-overview⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/kmO8X⟩) 'Gov.UK Verify hub'.

[689] Toby Stevens, *Gov.UK Verify Data Protection Impact Assessment* (v 1.0, Government Digital Service, GovUK Verify blog 2016) ⟨https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf⟩ accessed 20 July 2019 (archived at ⟨http://archive.fo/p73oW⟩) 10.

[690] ibid Glossary *"Relying Party"*.

[691] ibid 10.

[692] ibid 10.

[693] David Black, *"Validating identity information against an authoritative source"* (*GovUK Verify Blog*, 10 October 2014) ⟨https://identityassurance.blog.gov.uk/2014/10/10/introducing-the-document-checking-service/⟩ accessed 2 August 2019 (archived at ⟨http://archive.fo/ZRvnM⟩).

[694] Stevens (n 689) 10.

[695] GovUK Verify, *"Privacy notice"* (27 June 2018) ⟨https://www.signin.service.gov.uk/privacy-notice⟩ accessed 23 May 2019 [prior to last updated version of 18 June 2019]: *"This is done via an API and cannot be accessed by GOV.UK Verify."*

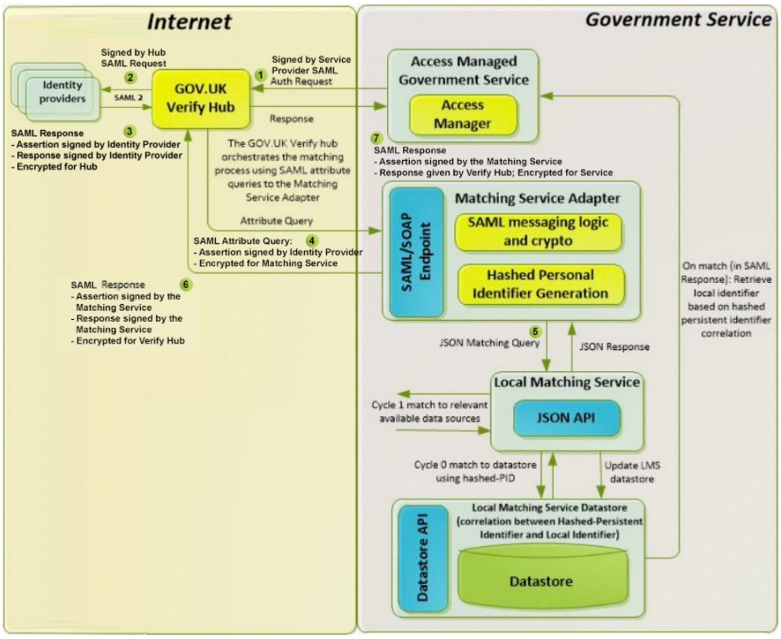

Internet
Government Service
Identity providers
Signed by Hub SAML Request
2
SAML 2
GOV.UK Verify Hub
1
Signed by Service Provider SAML Auth Request
Response
SAML Response
3
- Assertion signed by Identity Provider
- Response signed by Identity Provider
- Encrypted for Hub
The GOV.UK Verify hub orchestrates the matching process using SAML attribute queries to the Matching Service Adapter
Attribute Query
SAML Attribute Query:
4
- Assertion signed by Identity Provider
- Encrypted for Matching Service
SAML Response
6
- Assertion signed by the Matching Service
- Response signed by the Matching Service
- Encrypted for Verify Hub
Access Managed Government Service
Access Manager
7
SAML Response
- Assertion signed by the Matching Service
- Response given by Verify Hub; Encrypted for Service
Matching Service Adapter
SAML/SOAP Endpoint
SAML messaging logic and crypto
Hashed Personal Identifier Generation
On match (in SAML Response): Retrieve local identifier based on hashed persistent identifier correlation
5
JSON Matching Query
JSON Response
Local Matching Service
JSON API
Cycle 1 match to relevant available data sources
Cycle 0 match to datastore using hashed-PID
Update LMS datastore
Local Matching Service Datastore (correlation between Hashed-Persistent Identifier and Local Identifier)
Datastore API
Datastore

FIGURE 8.4: Gov.UK Verify actors and data flows[696]

The typical user journey in Gov.UK Verify starts when a user requests authentication to access a governmental service.

(1) The Service Provider sends an authentication request to the Hub (step 1, figure 8.4) indicating the requested LOA (at the moment Gov.UK Verify supports only LOA 1 and LOA 2).[697] The request is signed by the Service Provider. The Hub prompts the user to select one of the available Identity Providers, depending on the available data the user has for verification.

(2) An authentication request is sent to the selected Identity Provider, signed by the Hub (step 2, figure 8.4). The Identity Provider verifies the user's identity according to the indicated LOA.

(3) The verified identity is sent as a response to the Hub, signed by the Identity Provider (step 3, figure 8.4). The electronic identity contains an *"authentication assertion"* – encrypted for the Hub – which asserts that the user's identity is authenticated and contains contextual information including the LOA.[698] It also contains an 'Identity assertion', also encrypted for the Hub, containing two elements:

[696] as adapted from Identity Assurance Team, *Identity Assurance Documentation: Release* (2015) ⟨http://docplayer.net/21642604-Identity-assurance-documentation.html⟩ accessed 24 August 2019 (archived at ⟨http://archive.fo/US2UC⟩) 7–9.

[697] Government Digital Service, *"Understand the different levels of assurance"* (*GovUK Verify Documentation*, 7 January 2018) ⟨https://www.verify.service.gov.uk/understand-levels-of-assurance/⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/k2w3o⟩): *"It provides 2 different levels of assurance (LOAs) – LOA 1 and LOA 2. "* LOA 1 support was introduced after 2018.

[698] Government Digital Service, *"How SAML works with GOV.UK Verify"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/technology-overview/saml/#saml⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/wh1X6⟩).

the Matching Dataset and a Persistent Identifier. The Matching Dataset comprises of the same information for every electronic identity.[699] The Persistent Identifier is a pseudo-random value generated by the Identity Provider and refers to the combination of the user and the chosen Identity Provider.[700]

(4) The 'Identity assertion' is then sent by the Hub to the Matching Service located at the Service Provider. The 'Identity assertion' retains the signature of the Identity Provider and is encrypted for the Matching Service (step 4, figure 8.4).

(5) The Matching Service then performs a series of attempts to match the 'Identity assertion' to a local user record, known as 'matching cycles'. The first cycle, 'cycle 0', starts when the Matching Service changes the Persistent Identifier to a hashed value, created from the combination of user, Identity Provider and Service Provider.[701] After creation of the hashed persistent identifier, the Matching Service looks up a local datastore to see if the same hashed value exists associated with a local record. If a match is found, the 'Identity assertion' along with the hashed identifier are forwarded to the Service Provider. If not, the Matching Service tries to determine a match using the values of the matching dataset ('cycle 1'). Subsequent cycles, if no match is found, ask the user for additional attributes.

(6) When a match is found the Matching Service sends a 'match' response along with the 'Identity assertion' back to the Hub, signed by the Matching Service and encrypted for the Hub (step 6, figure 8.4).

(7) The Hub sends the signed 'Identity assertion' in an encrypted form to the Service Provider (step 7, figure 8.4), which then retrieves the local record from its database.

[699] Government Digital Service, *"Data from GOV.UK Verify"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/using-verify-data/data-from-verify/#data-from-gov-uk-verify⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/Jv8zF⟩).

[700] ibid 'Persistent identifier'.

[701] ibid 'Persistent identifier': *"The Verify Service Provider will hash the PID to make it specific to each service"*.

Opt.[a]	**eIDAS MDS**	**Gov.UK Verify Matching Dataset**
M	Uniqueness identifier	Persistent identifier[b]
M	Current family name(s)	Family name
M	Current first name(s)	First name
M	Date of birth	Date of birth
O	First name(s) and family name(s) at birth	—
O	Place of birth	—
O	Current Address	—[c]
O	Gender	—

[a] *M* = Mandatory attribute, *O* = Optional attribute

[b] The identifier is persistent per pair of user ⟷ Identity Provider (IdP). Since users can hold accounts with different Identity Providers, multiple persistent identifiers for the same natural person may exist.

[c] The ⟨`current address`⟩ field is present in the list of attributes held by the Identity Provider(s). However, it is not disclosed as part of the eIDAS Minimum DataSet.

Table 8.2: Minimum Data Set provided by the Gov.UK Verify[702]

Some remarks must be made regarding Gov.UK Verify's design, and in particular in relation to Verify's participation in the eIDAS Interoperability Framework. Although the European Commission has issued a notice of withdrawal of the UK from eIDAS,[703] in light of Brexit, the extent of the participation of the UK in the Single Market is still under negotiation. Presently, the UK stopped being an EU member on 31 January 2020.[704] A transition period to decide on the future relationship has been agreed in a *"Withdrawal Agreement"*[705] and accompanying *"Political declaration"*.[706] The transition period is due to end on 31 December 2020. All EU law applicable to the UK at the time of exit continues to apply during the transition period.[707] eIDAS is in effect in

[702] Agency for Public Management and e-Government (n 683) 23.

[703] European Commission, *Notice to Stakeholders: Withdrawal of the United Kingdom and EU Rules in the Field of Electronic Identification and Trust Services for Electronic Transactions* (2018) ⟨https://ec.europa.eu/info/sites/info/files/notice_to_stakeholders_brexit_e_signature_final.pdf⟩ accessed 14 April 2019 (archived at ⟨http://archive.fo/uYlcw⟩).

[704] Previously, the European Union (Withdrawal) Bill 2017-19 set as the 'exit day' the 29th of March 2019, before its last amendment at the House of Lords that removed the reference to a specific date. Since, the UK and the EU agreed to an extension of the process until the 31 October 2019 (Katya Adler, *"Brexit: UK and EU agree delay to 31 October" BBC News* (London, 11 April 2019) ⟨https://www.bbc.com/news/uk-politics-47889404⟩ accessed 20 May 2019 (archived at ⟨http://archive.fo/3DALG⟩)) and a later extension until 31 January 2020.

[705] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (United Kingdom—European Union) (adopted 19 October 2019, signed 17 October 2019); ratified and incorporated into UK law by European Union (Withdrawal Agreement) Act 2020.

[706] HM Government, *Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom* (2019) ⟨https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840656/Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2ZEFw6f⟩).

[707] Withdrawal Agreement (n 705).

the UK until the end of the transition period.[708] Gov.UK Verify was pre-notified on 28 August 2018 and, after a peer-review, has been accepted in the list of notified schemes under eIDAS Article 9(1) on 2 May 2019.[709] National legislation[710] has been enacted to implement the penalties outlined in eIDAS and identify the supervisory body, i.e. the UK ICO.[711] The GDPR has been incorporated into domestic law under section 3 of the Withdrawal Agreement Act 2018.[712] Therefore, the discussion that follows is not only relevant for EU schemes of a similar architecture, but apply to the UK insofar as it is still a Member State.

First of all, concerns had been expressed in the literature[713] about the LOA2 which was, at the time, the only level of assurance supported by Gov.UK Verify.[714] According to the information published at the time, it would seem that LOA2 would correspond to the eIDAS LoA *"Low"*, which would mean that recognition of Gov.UK Verify by other Member States would only happen on a voluntary basis.[715] However, during the notification peer review, the UK has provided further details on the registration and authentication requirements for LOA1 and LOA2 (table 8.3). The review committee, therefore, accepted that *"[t]hese requirements [...] can be mapped for identity levels 1 and 2 to eIDAS LoA Low and Substantial respectively"*,[716] but with objections.[717]

[708] eIDAS does not extend the adequacy provisions for trust services to eID services. Under the notice of withdrawal, the EU notes that by default the UK's eID scheme will no longer be recognised in the Internal Market: European Commission, *Notice to Stakeholders: Withdrawal of the United Kingdom and EU Rules in the Field of Electronic Identification and Trust Services for Electronic Transactions* (n 703) 2.

[709] Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2019] OJ C150/11.

[710] Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, 2016 No. 696.

[711] The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016.

[712] European Union (Withdrawal Agreement) Act 2018, s 3 as amended by Withdrawal Agreement Act 2020. For a discussion about the future evolution of data protection in the UK after Brexit, see Paul de Hert and Vagelis Papakonstantinou, *"The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit"* (2017) 33(3) Computer Law & Security Review 354 DOI: 10.1016/j.clsr.2017.03.008, 359–360.

[713] For a discussion on these concerns, see Tsakalakis, O'Hara, and Stalla-Bourdillon (n 643); Tsakalakis, Stalla-Bourdillon, and O'Hara, *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (n 643).

[714] See n 697.

[715] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73, art 6(2).

[716] Agency for Public Management and e-Government (n 683) 18. For the level *"Substantial"*, Gov.UK Verify satisfies Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/7, art 2.1.2 points 1 and 2.

[717] Agency for Public Management and e-Government (n 683) 20 and 35: *"There was concern among peer reviewers as to whether processes in place were sufficient to verify that non-UK documents are genuine"*; *"One Member State found that for some enrolments where remote identification through an app is based on static images, the UK scheme does not fulfil all requirements for LoA substantial."*

Secondly, even though Gov.UK Verify aims to comply with privacy-by-design and minimisation principles, as noted in its Identity Assurance Principles,[718] certain design choices appear inconsistent with these premises. Implementation of the Hub in between Identity Providers and Service Providers aimed to guarantee unlinkability – that a user cannot be associated with a particular eID means and the different activities of an eID means cannot be associated with each other. Unlinkability is mandated by the Assurance Principles of *"Minimisation"* and *"Transparency"* that form the regulating policy of the whole scheme.

Between the Identity Provider, the Hub and the Matching Service, electronic identities are exchanged in the form of a record with a set amount of attributes. The record contains a PersistentID, in the form of a hashed value constructed from the identifiers of the Identity Provider and the user, and a matching dataset, comprised of the first and last name, the date of birth, and optionally the address and gender.

Gov.UK Verify does not seem to support selective disclosure.[719] It is safe to assume that the matching dataset is always transferred to and from the Hub. On top of the original identifiers, the matching dataset will be enriched by user provided attributes, in case of a failed attempt to match the local records.[720] It is noteworthy that in cross-border transactions, the Minimum DataSet that Gov.UK Verify transmits will be comprised of only full name, date of birth and the persistent identifier. Since the identifier is different for each Identity Provider, if a user has subscribed to more than one Identity Providers,[721] foreign electronic services will have no way of distinguishing whether the two records belong to the same or different natural persons.[722] The eIDAS Cooperation Network in its peer review of Gov.UK Verify encouraged the UK to enrich the Minimum DataSet that will be transmitted with additional attributes.[723]

[718] Privacy and Consumer Advisory Group (n 684).

[719] Luís Brandão, Nicolas Christin, and George Danezis, *"Toward Mending Two Nation-Scale Brokered Identification Systems"* (2015) 2015(2) Proceedings on Privacy Enhancing Technologies 135 DOI: 10.1515/popets-2015-0022, 147.

[720] The specification requires additional user consent to be given in case an attribute provider is involved to enrich the matching dataset, with user consent assumed since the user is the source of the attributes. The Central Hub is forbidden by policy to store any other information than the matching dataset and the association of pseudonyms: Cabinet Office, *Identity Assurance Hub Service SAML 2.0 Profile v1.2a* (2013) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458610/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf⟩ accessed 23 July 2015 (archived at ⟨https://tinyurl.com/ybqjmo9h⟩) 23.

[721] Agency for Public Management and e-Government (n 683) 23: *"the UK user may have multiple eIDAS identifiers for cross-border authentication depending on the IDP he/she is using."*

[722] ibid 23: *"The minimum data set contains only an eIDAS identifier, date of birth and name – thus it might be hard for relying parties to know when two log-ons,with the same combination of date of birth and name, but with different eIDAS identifiers, stem from the same person, and when they do not. Additional attributes may be needed to reliably link the identifiers of the same person."*

[723] ibid 27–28: *"However,the UK's minimum data set includes only the eIDAS identifier, name and date of birth. For first time recognition (when the eIDAS identifier is unknown to the relying member state) or for data sets that differ just in the unique identifier (which can be the same person using different IdPs, or two different persons) this data set might be insufficient to correctly recognise the person within the member state's records.* ***The peer reviewers encourage the UK to enrich the minimum data set with further information, e.g. by including the person's place of birth."*** [emphasis given].

An alternative to disclosing further attributes might lie in the way the Matching Service is deployed within the Interoperability Framework. After a successful authentication, the Matching Service creates an association table, storing the pseudonym and the local identifier of the Service Provider together. The pseudonym assigned by the Matching Service is persistent. This is in order to avoid having to follow the same process every time: the Matching Service needs to associate the account from the Identity Provider to a local one only the first time; by keeping the pseudonyms static each subsequent time the Matching Service knows to which local account the eID means refers to. But this also means that if more than one Service Providers access the same Matching Service, they will all receive the same pseudonym for each eID means. Since the Matching Service is deployed at the Service Provider level, there is no telling of how many different Matching Services exist. If the same pseudonym assigned to a user is shared by more than one Service Provider, it effectively allows the pseudonym to function as a *de facto* unique identifier.[724] Conversely, if all cross-border authentications would go through the same instance of the Matching Service, the pseudonym would remain static for all Service Providers. An example of how such a deployment could work in an eIDAS setting can be seen in figure 8.5.

Therefore, even though Gov.UK Verify supports pseudonyms it restrains their use as a *de facto* identifier; by not allowing for selective disclosure of attributes it is highly unlikely the scheme would be able to produce pseudonymous datasets (at least by the GDPR's definition), raising questions as to its compliance with the GDPR and, ultimately, eIDAS. Notably, the government has indicated that it is looking to outsource the Hub component to private-sector companies.[725] Considering the prime position of the Hub in a Verify authentication (the Hub receives, even just in passing, the whole matching dataset and all persistent pseudonyms) it is questionable whether the current level of unlinkability will be suitable if the Hub is bought by the private sector.

8.5 Impact of the Interoperability Framework on National eID Schemes

All three national eID schemes analysed here have been developed with the intention to meet privacy and data protection by design requirements, even if their creation is prior to the entry into force of the GDPR and its application.

The foregoing analysis is indicative of the state of the art as regards the protection goal of unlinkability. Indeed, it can be observed that the goal of unlinkability plays an integral

[724] Brandão, Christin, and Danezis (n 719) 320.

[725] David Bicknell, *"Brexit brake on Verify spurs GDS to woo private sector on digital identity"* [2018] Government Computing ⟨https://www.governmentcomputing.com/brexit-eu/news/brexit-brake-verify-progress-spurs-gds-woo-private-sector-digital-identity⟩ accessed 30 April 2018 (archived at ⟨http://archive.fo/ZdTOj⟩) .

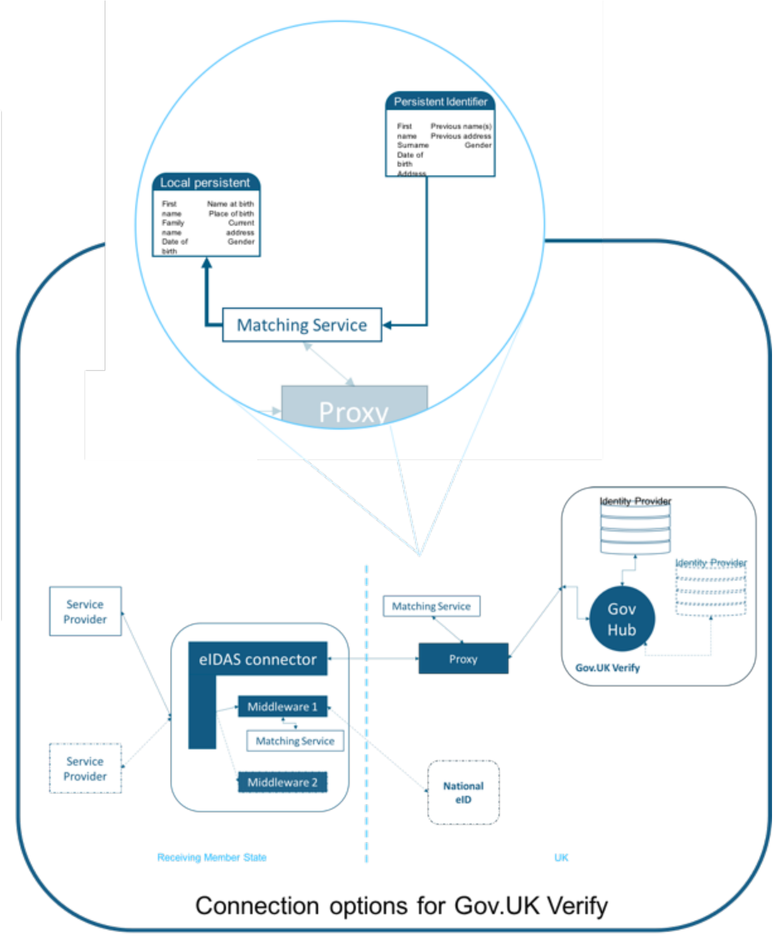


FIGURE 8.5: Gov.UK Verify proxy deployment inside the Interoperability Framework

role in how electronic authentication is defined in all case studies. The three schemes analysed all employ a mix of technical and organisational controls to effect unlinkability:

Organisational controls are mainly used as a preventive measure to effect unlinkability against the aggregation of excessive personal data (in other words, unlinkability as data minimisation and purpose limitation). The strongest evidence of this use is in Germany, where data aggregation is forbidden via hard legal instruments.[726] Softer versions can be found in Austria and the UK, where equivalent prohibitions exist in soft policy instruments.[727] On the other hand, unlinkability as the obfuscation of a user's activities to prevent profiling is effected through technical controls. Although to different degrees, pseudonymisation is engineered into all three systems. In Austria, pseudonyms are constructed based on the derivatives of the sPIN of a natural person and the sector-specific identifier of the public service. In the UK, an analogous use sees a pseudonym constructed by hashing a combination of a natural person's, an Identity Provider's and a Service Provider's identifier. In Germany, nonsensical pseudonyms can be constructed on the fly for each different use. The pseudonymisation functionality

[726] See n 669.

[727] See nn 646 and 684.

	eIDAS LoA	**STORK 2.0** QAA	**Austrian ACC**[728]	**German nPA**	**Gov.UK Verify**	Example
Levels of Assurance	N/A	N/A	N/A	N/A	N/A	Anonymous submission of a form.
	N/A	1	N/A	0	0	Opening an e–mail account. The account only verifies that an email address exists.
	'Low'	2	N/A	1	1	Online account with an electricity provider. The account only verifies that it relates to an actual electricity meter.
	'Substantial'	3	N/A	2	2	Paying online. The account only verifies (a) the user holds a valid bank card and (b) the bank account associated with the card will be used.
	'High'	4	N/A	3	3 (not currently supported)	Using an ePassport to enter a country. The electronic terminal verifies that (a) the credentials relate to a valid identity and (b) the identity belongs to the person presenting the ePassport.
	N/A	N/A	N/A	N/A	4 (not currently supported)	Performing electronic transaction with minimum risk of identity impersonation. The eID means used verifies that the identity is existing, genuine and valid and its biometric information matches the biometrics of the holder.[729]

Table 8.3: Mapping of national assurance levels to STORK and eIDAS [as adjusted from table 3.1]

in Germany is enhanced by advance data minimisation through selective disclosure of attributes. The German scheme is the only one, thus, that can currently produce truly pseudonymised datasets in the meaning of GDPR Article 4(5). However, the update on the Austrian scheme that is currently in the works is expected to introduce similar functionality.

Considering the impact that the Interoperability Framework will have in the operation of the three schemes, by combining the analysis of chapter 8 with eIDAS as explained in chapters 3 and 4, the following observations can be made:

8.5.1 The ACC

Domestically, the ACC assigns different ssPINs according to the sector of the Service Provider. However, foreign Member States do not necessarily follow the breakdown of sectors in a similar fashion to Austria. Accordingly, Austria will be unable to assign different ssPINs to different Service Providers – instead the most probable scenario is to assign one ssPIN per Member State, with all Service Providers under that Member State receiving the same ssPIN. In terms of selective disclosure, and before knowing its precise implementation, the accompanying dataset that Austria currently deploys in eID

[728] Austria has not yet released any public plans to notify ACC.

[729] Note that this Level and its description is based on the guidance for Gov.UK Verify (Government Digital Service, *Good Practice Guide (GPG) 45: Identity proofing and verification of an individual* (v. 4.1.1, 2019) ⟨https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual⟩ accessed 9 September 2019 (archived at ⟨http://archive.fo/a3bLF⟩) s 9.4). In the original analysis, before Verify's notification process, Verify's LoA 1–4 were aligned to STORK's QAA 1–4. However, since the notification review process accepted that Verify's LoAs 1 and 2 correspond to eIDAS' 'Low' and 'Substantial', the allocation of Verify's LoA 4 has been accordingly modified.

transactions is similar to eIDAS' Minimum Dataset since it contains the same attributes as the Minimum Dataset's mandatory part. The strain put by the Interoperability Framework will most likely have to do with this set of attributes being accompanied by a persistent unique identifier, for all intents and purposes, making easier therefore the possibility of linkability compared to the different ssPINs that the scheme currently uses.

8.5.2 The NPA

The nPA will have to assign permanent pseudonyms *in lieu* of unique identifiers to German citizens transacting with foreign Member States. The pseudonymisation function will act quite differently from what happens in domestic eID transactions: Although Service Providers in Germany receive each a different pseudonym, all Service Providers under a foreign Member State will be receiving the same pseudonym for each user. Additionally, the ability to select which attributes to transmit to Service Providers will be limited, since the mandatory attributes of the Minimum Dataset have to be included in every transaction at the cost of the authentication failing.

8.5.3 The Gov.UK Verify

For Gov.UK Verify much of the outcome of participating in the Interoperability Framework will have to do with the way the Central Hub and the Matching Service will be deployed to the foreign Member States. Since unlinkability between the Identity Provider and the Service Provider is based on the ability of the Hub to mediate the transaction and the capability of the Matching Service to disguise the pairwise-persistent[730] pseudonyms that the Identity Providers send, the level of unlinkability will depend on how many instances of the Hub and the Matching Service will exist. If the Matching Service is installed at the level of the Service Provider, every Service Provider will receive a different pseudonym. However, an implementation like this will probably in practice be impossible to achieve and maintain. If the Matching Service is installed at the level of the Member State, the pseudonym will remain the same for all Service Providers of a given Member State. If instead the Matching Service is deployed centrally in the UK, all Member States and their Service Providers will be receiving the same pseudonym. Conversely, in both cases, the pairwise pseudonyms created from the Identity Providers will always be transmitted through the Hub until they reach the Matching Service. However, at least in theory, the possibility to possess different eID means in different Identity Providers increases the variety of pseudonyms a user can enjoy, since its pseudonym is constructed in part based on the selected Identity Provider.

[730] Pairwise-persistence signifies that the identifier remains the same for the particular pair of sender – recipient: OASIS (n 655) s 3.4.2.

8.6 Conclusion

This chapter examined three national eID schemes. The three schemes are built around different architectural models: the Austrian ACC is a federated eID scheme that relies on a central data register; the UK Gov.UK Verify is a federated eID scheme of a 'hub-and-spoke' configuration where a hub mediates communications across multiple Identity Providers; finally, the German nPA is a user-centric system where the role of the Identity Provider lies with the citizen who communicates directly with the Service Providers. Each eID scheme has in place different unlinkability safeguards.

The most advanced in terms of features and user control is the nPA. The nPA allows the German citizens to select which attributes to disclose in each authentication. Further, it provides on-the-fly creation of pairwise pseudonyms. And it is able to mask attributes of residence or date of birth by providing yes/no attestations.

The ACC does not currently support selective disclosure, although plans to implement this functionality are being discussed. It does, however, support pseudonymous identifiers in the form of sector-specific pairwise identifiers. To compensate for any risks arising from the permanence of the sector-specific identifiers, the Austrian DPA, who is the supervisory body, has enacted strict rules of the entities per sector that can have access to the eID data. The level of access is layered per sector and per entity's needs.

Finally, Gov.UK Verify uses a form of pairwise pseudonym creation which coupled with the ability to create eID means with multiple Identity Providers is hoped to alleviate risks of linkability. Selective disclosure is not supported. However, as discussed, there are inherent risks in the way Gov.UK Verify handles pseudonyms that lie with the position of power that the Hub is in and the way pseudonyms are communicated to the Service Providers. In a scenario where a sole Hub exists and multiple Service Providers use the same instance of the Matching Service, the same pseudonym will be deployed across all Service Providers. In such a scenario, in essence, Gov.UK Verify runs the same risks of linkability that the Minimum Dataset and the unique identifier create for eIDAS' Interoperability Framework.

It should be recognised, however, that all of the examined eID schemes present pseudonym creation as a bare minimum towards satisfying the unlinkability goal. Where pseudonymisation is not accompanied by selective disclosure, the risks of rendering pseudonymisation meaningless are mitigated through policy measures. Notably, though, the policy measures are effective on a national level. A notification of the schemes for use within the Interoperability Framework will not extend the application of the policies, whether in the form of national laws (as in Austria) or in the form of codes of practice (as in the UK), to the receiving Member States.

As a result, it becomes clear that participation of the schemes in the Interoperability Framework will offer a weaker data protection by design level. In the case of Austria and the UK, the pseudonymous identifiers will take the place of a (persistent) unique identifier that will remain constant across all receiving Member States. In the case of Germany, nPA will not only lose the ability to create on the fly different pseudonymous identifiers but also the abilities of selective disclosure and masking.

Participation in eIDAS, therefore, results in practice in a reduction of the level of data protection guaranteed by national eID schemes. This makes it difficult to argue that eIDAS Article 12(3)(c) is complied with by the current specifications of the Interoperability Framework. It also puts national data controllers (i.e. Identity Providers and operators of eID schemes) in a difficult position to demonstrate compliance with GDPR Article 25 and can have implications in terms of liability despite eIDAS Article 11.

In order to confirm the foregoing analysis of the impact of eIDAS on national schemes, as well as the limitations of unlinkability in the Interoperability Framework, the following chapter performs a qualitative analysis of data collected in the context of semi-structured interviews with experts in the field of eID.

Chapter 9

Expert data analysis

Taking into account [...] the nature, scope, context and purposes of processing...
— GDPR Art 25(1)

9.1 Introduction

This chapter presents the qualitative data analysis performed on a series of short interviews with eID experts.[731] The interviews had a semi-structured format, using an interview guide with open-ended questions as a starting point. The data analysis is being used as part of the triangulation of methods to scrutinize the findings of the previous chapter in relation to the importance of unlinkability, to investigate the ways to meet this goal by national eID schemes and to assess the prospects of a practical application to increase the level of unlinkability supported by the Interoperability Framework.

Section 9.2 defines the methodology that was used during the interviews and section 9.3 discusses the themes that emerged out of the analysis of the interviews. The material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness.*[732] Part of the material was published under *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[733]

[731] Appendix B.

[732] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[733] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

9.2 Interview Methodology

Interviewees were selected through expert sampling, based on their experience in the architectural or policy design of national eID schemes and their familiarity with eIDAS. Although it is suggested that usual sample size for semi-structured interviews should be around 20 to 30 participants to reach saturation,[734] for studies with a high-level of homogeneity, like the field of national eID technology, a much smaller sample should be sufficient for identifying meaningful themes and producing useful interpretations.[735] Out of 18 Member States with eID schemes under a notification process,[736] interviews were conducted with experts from 6 countries. The six countries represented the two thirds (2/3) of EU Member States with notified eID schemes at the time of recruitment.[737] Five of the six Member States have already completed the notification process of their eID schemes under eIDAS Article 9.[738] The participants were allowed to diverge from those questions and focus on the topics they best considered important for Data Protection by Design and privacy features in eID schemes. Selection criteria for the participants were based on expertise and involvement within national initiatives: eligible participants should have worked for or with a national eID scheme of one of the countries within the scope of eIDAS. This means that eligible countries were Member States of the EU or the EEA. Each interview began with a brief overview of the national scheme, after which more focused questions followed. A sample of the interview guide can be found in appendix C. The experts were asked to define Data Protection by Design according to their understanding and comment on the Data Protection by Design features that national schemes have implemented. Finally, they were asked to comment on the Interoperability Framework and its impact on the national schemes in terms of privacy. A solution to support a greater level of unlinkability was proposed to them. They were requested to consider whether it would offer an improvement over the current implementation, taking into account the the cost of implementation.

9.3 Emerging Themes

Overall the interviews confirmed not only that there are differences between the national schemes, but that the attitudes towards protected data vary from country to country.

[734] Greg Guest, Arwen Bunce, and Laura Johnson, *"How many interviews are enough? An experiment with data saturation and variability"* (2006) 18(1) Field Methods 59 , 61.

[735] The authors seem to propose that in most cases a sample size of 6 would be enough to reach saturation: ibid 78.

[736] At the moment of writing in 5 Member States the notification process is still ongoing: See Denmark, Lithuania, the Netherlands and Portugal in *"Country overview"* (*CEF Digital*, 2019) ⟨https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview⟩ accessed 12 September 2019 (archived at ⟨http://archive.fo/8tDw2⟩).

[737] See archived version of ibid.

[738] Portugal has completed the notification process for its eID card scheme (*"Cartão de Cidadão"*) and the private-sector *"Chave Móvel Digital"*, whereas one other (the scheme for professional qualifications *"Sistema de Certificação de Atributos Profissionais"*) is under notification currently: ibid.

Although in all countries the data that comprise the Minimum Dataset, i.e. first and last name, date of birth, current and previous address, gender and any previous names, are considered worthy of protection, the level of protection varied significantly. In Estonia, for example, the data are considered public and not in need of any further privacy protection.[739] Deployment of the identifiers is logged and can be traced by interested parties, i.e. the user, the Identity Provider and the authorities. This is seen, to the expert, as a means to offer transparency to the citizens.[740] In Portugal, the name and date of birth are easily readable from the eID, whereas the address requires prior authorisation.[741] In the UK, even though all three fields – name, date of birth and gender when provided – are encrypted, their presence in the dataset is considered necessary for the business purposes of both public and private sector providers.[742] The necessity of the dataset for business purposes was also highlighted in the Estonian interview.[743]

Similar attitudes were noted in the case of unique identifiers. Although in Estonia the unique identifier used contains some personal information (namely the date of birth and gender),[744] it is considered as public data and therefore used freely. The same format is being used for the national number embedded in the electronic certificates in Belgium, however the expert was sure to highlight that its use should be seen as problematic as it can lead to linkability risks and involuntary data disclosure.[745] In Portugal, although sector-specific identifiers are constructed to avoid the use of a unique identifier, these sector-specific identifiers are freely readable from the eID. In addition, the information embedded in the electronic certificates poses a threat to unlinkability, as it can be used to profile the users.[746] Sector-specific identifiers are also employed in Austria, and are called

[739] *"In our case the data we use for authentication in terms of eIDAS, this data is concerned more or less. It's not anywhere written that it's public data, but it's handled as it should be handled as a public data."* appendix B lines 1218–1219.

[740] *"So you get like dots and lines between them, so you can see directly and this is also publicly available. So this is another measure for transparency, people have a right to know."* appendix B lines 1118–1119.

[741] *"... the data file that contains the same information that is printed on the card [...] That can be read openly, as long as you introduce the card in a smartcard reader. And there's also another separate data file with the address and the address is protected by a PIN code."* appendix B lines 1628–1629. A distinction made also in the Estonian interview but in relation only to the eIDAS dataset.

[742] *"But it's not a huge privacy risk and the number of services that would not want to, for example, personalise it by your first name is fairly limited realistically in a competitive marketplace at the moment with current privacy attitudes"* appendix B lines 1863–1866.

[743] *"... in eIDAS there are minimum set of data. It can't be handled as private data or protected data because if you handle it like that the cross-border authentication will never work. If you handle eIDAS minimum data as private, cross-border authentication will never work."* appendix B lines 1272–1274; *"Absolutely, it's necessary, absolutely necessary. If you build your system that doesn't take this into account then you are in the big trouble. So minimum set of data should be considered as public data or data that cannot be controlled as a private data."* appendix B lines 1280–1283.

[744] *"Because this number is not impersonalised, this number consists of some personal data. It consist of which century and if you are a male or female then it has also your birthdate and then there are other numbers, control numbers that makes it unique."* appendix B lines 1017–1020.

[745] *"But it at least contains your national register number, which is the source of any potential privacy violation. This is the Belgian government identity number that you have, the primary number one and it's in the certificate."* appendix B lines 569–572; *"Linkability is technically feasible and legally forbidden"* appendix B lines 745–748.

[746] *"Yes, there are some risks. [...] so whenever you use the card or certificate for authentication in a website, that can be collected from the website."* appendix B lines 1666–1671.

ssPINs; the ssPINs were previously in the physical control of the user, however a move to a model where the ssPINs are stored centrally with the Data Protection Authority is forthcoming. It was highlighted in the interview, that the move carries some privacy risks but these are mitigated by additional legal controls. Even though tight legal controls are in place in Germany as well, technological controls ensures unique identifiers are substituted with pseudonyms.[747] Semi-persistent pairwise pseudonyms are employed by the UK as well, with a central hub in charge of substituting the pseudonyms received by the Identity Provider before they reach the Service Provider.[748]

In terms of privacy controls for the national schemes, in both the cases of Germany and Austria the importance of strong technical controls was highlighted. The most prominent controls were to do with two features: how the schemes handle a unique identifier and the disclosure of data that serves three functions – data security, data minimisation and transparency towards the purposes of processing. The strongest controls in relation to unique identifiers seems to be the pseudonymisation functionality in the German scheme. The ssPINs serve a similar function in Austria, however the move towards a scheme with a centralised Identity Provider (the sPIN Authority) introduced some compromises to the effectiveness of the control. The ssPIN is thus complemented by the end-to-end encryption of the assertions created by the scheme.[749] A new feature that will allow users to track which of their attributes have been transmitted by the scheme is in the works.[750] Even with strong technical controls in place, in both interviews the importance of legal controls that limit how the technology can be exploited was highlighted.[751] Legal controls as a measure to offset misuse of personal data was brought up in the Belgian interview, because of the scheme's use of the national number as an embedded identifier. However, the effectiveness of these legal controls was questioned:[752] in order to perform the authentication, the scheme needs to store the identifier for a short period of time, after which the identifier is deleted. However, storing the identifier is forbidden by law in Belgium. Hence, to perform authentication the scheme has to violate the legal controls,

[747] *"Absolutely. This is... from a privacy perspective, I think, the German system. if you only look at security and privacy this is exactly how you would design a system. But from a practical point of view, the downside of this approach is that it's a little bit over engineered?"* appendix B lines 1457–1460.

[748] *"it's limited visibility rather than complete unlinkability, just from the way these things end up getting built."* appendix B lines 1910–1911; *"So [name] using the same Identity Provider to log onto two government services will have two of those unique semi-persistent identifiers."* appendix B lines 1939–1940.

[749] *"So in the new architecture, for instance, attribute provisioning gets more complex technically, as to maintain the same level of data protection."* appendix B lines 37–39.

[750] *"What we could introduce is that the citizen herself can see the locks so that she can access all her eID activities, and... To see whether there was any compromise, or the card she lost, together with her pin probably, was used in a service."* appendix B lines 419–420.

[751] *"Again there are legal measures that that those data may only be stored for displaying that to the user, to see the history. But basically as in any identity system that uses the Triangle IDB Service Provider and user, unless you have processing at the user device, somehow learns who is the Service Provider."* appendix B lines 337–341.

[752] *"This is total mismatch between technical reality and legal implementation."* appendix B lines 620–621.

even if for a short period of time. Policy measures were also the controls used to mitigate any risks out of the central components used in the Estonian scheme.[753]

The feasibility of relying on legal controls in a cross-border setting was challenged in a number of interviews. It was highlighted that national controls work in the context of a sovereign State, but Member States who notify their national schemes have no power to enforce controls to other Member States.[754] Therefore, there is no guarantee that the national scheme will have the same protections when operated across borders.[755]

The shortcomings of the Interoperability Framework were highlighted in relation to technical controls as well. For schemes that support sector specific identifiers, participation to the eIDAS Interoperability Framework will force them to assign uniform identifiers per receiving Member State.[756] This is due in part to the inability to control if foreign public services are divided into sectors[757] but also because of the mandatory presence of a *"uniqueness identifier"* in the Minimum DataSet.[758] The presence of the Minimum DataSet was also viewed as forcing in practice the schemes to perform identification,[759] whereas certain needs could be served by authentication which requires the disclosure of less data. However, in some cases this was viewed as a necessary compromise for interoperation.[760]

A common theme among all the expert interviews was the need to distinguish between Service Providers in the public sector and Service Providers in the private sector.[761] Admittedly eIDAS is mandatory for public-sector providers only, but since voluntary

[753] *"... we can see which country is using it, but not we can see in detail. Inside in Estonia we can see on base of IP address. Because you see, when authentication is done then the OCSP request is sent if it's certificate is valid or not. And this request stores from which IP address the request was done, so if it's some web shop, the web shop makes this query and they see the web shop IP address."* appendix B lines 1380–1385; *"Certain databases are publicly available [...] Some databases have really strict rules, like health records [...] those are most controlled databases and there are a lot of strict rules and regulations around them"* appendix B lines 1132–1136.

[754] *"It is up to the sending and receiving member state what protocols, what security measures are deployed nationally."* appendix B lines 419–420.

[755] *"... only one persistent identifier within Belgium is having a lot of privacy risks. And if you would use that to reach out to the 27 other Member States, that would only make things worse. Now, because you can do more linkage..."* appendix B lines 724–727.

[756] *"... for example the eIDAS node in Spain will become one Service Provider and it's... the eID card will produce a pseudonym which is tied to Spain. And of course the privacy, if you only consider the privacy aspect somewhat decreases, in theory at least."* appendix B lines 1491–1494.

[757] *"Under the territorial principle already under the data protection directive, we however cannot impose that identifier, for instance in UK, also is derived sector specific."* appendix B lines 172–174.

[758] *"eIDAS to some extent is hindering it through the as persistent as possible clause, because if I then derive per Service Provider, it... I wouldn't do my best the possible in terms of persistence."* appendix B lines 496–498; *"the conclusion would be that eIDAS is not in line with [Data Protection by Design], because the Minimum Data[set]"* appendix B lines 1533–1534.

[759] *"They are rather driving eIDAS in the direction of using electronic identification"* appendix B lines 766–766; *"... this set of three attributes together can promptly give you quite some linkability. So you can have a brilliantly specified unique identifier persistent as possible in time, which is a pseudonym, but then the results that if you try to link queries."* appendix B lines 745–748.

[760] *"of course standardisation and collaboration on a European scale requires that a different member states and cultures somehow move together."* appendix B lines 1509–1511.

[761] *"I would, however, a bit distinguish here between public services, and private sector services."* appendix B lines 433–434.

recognition from the private sector is possible and since most of the national schemes are used domestically to access public and private sector Service Providers, future involvement of the private sector in eIDAS was deemed expected. It seems that the prospect of disclosing data to the private sector is regarded with more hesitation than when the Service Provider is of public nature.[762] This is partly because of the perception that governmental Service Providers offer more guarantees in terms of compliance with the purpose limitation principle. In some cases, this was accompanied by the perception that the public sector already shares, or has the ability to share, data between services,[763] so disclosing the minimum dataset would not increase risks of profiling the users. Also, it was a common understanding that most public services rely on all the identifiers present in the minimum dataset to be able to distinguish between individuals.[764]

Private sector Service Providers differ, according to the experts, because there are more use cases where the transactions can be performed with less data.[765] An example given was the sale of goods where the only information needed to complete the transaction is that the customer is human and of legal age. However, the opposite view was also expressed – stating that the mandatory presence of the Minimum Dataset attributes is not necessary even for public-sector services.[766] It is in these cases that the eIDAS Interoperability Framework could benefit from the implementation of technical controls, like selective disclosure and pseudonymisation.[767] Pseudonymisation would mitigate the risk of persistent identifiers and allow advanced schemes to create more robust non-persistent pairwise identifiers. Selective disclosure would permit a selection amongst the identifiers of the Minimum Dataset, so that private-sector Service Providers do not receive any data beyond their purposes of processing. In fact, pseudonymisation and selective disclosure might be considered fundamental ingredients for data protection by design.[768]

[762] *"I think if I was driving policy I would say what Facebook really wants is attributes."* appendix B lines 2288–2288.

[763] *"Well, they've also got the data anyway."* appendix B lines 1989–1989; *"I guess in many member states, the name and date of birth is used in most public services."* appendix B lines 437–438.

[764] *"So maybe it makes sense for public administration services or government services to have a minimum data set. But for private sector it should be, well, defined if there's cases by basis."* appendix B lines 1737–1739; *"But those services that we are mainly looking at as the early adopters, need that minimum data anyhow."* appendix B lines 449–450.

[765] *"In the case of shopping, e-commerce, you may want more privacy, but that's just because the use cases are very different."* appendix B lines 774–776; *"I think of many services that will only think they need this email. They don't even need to know your name or ID. So I think [eIDAS] that's mostly focused on public administration services."* appendix B lines 1724–1726.

[766] *"You can establish a system where you only have identifiers between the different applications and if there is a need to provide the name and additional attributes this can be user-centric."* appendix B lines 1576–1578.

[767] *"by stating a minimum data set, we are actually narrowing the scope of services [eIDAS can be used on] or expanding, actually expanding the data set"* appendix B lines 1734–1735.

[768] *"I think if you consider what Privacy by design in identity management means there are good reasons to exactly put the requirement for the application of sector specific pseudonyms and selective disclosure, it's actually a must."* appendix B lines 1527–1530.

Implementation of selective disclosure and pseudonymisation should be technically feasible according to the experts.[769] In fact, one of the experts argued that such a possibility had been discussed in the eIDAS Technical Subgroup, but was abandoned until eIDAS gains enough traction amongst the Member States.[770] However, most experts, when asked if a solution that will implement selective disclosure and pseudonymisation at the point of the eIDAS nodes would be desirable, agreed that it would be of value for the privacy of the national schemes.[771] Such functionality could be added in the form of a Regulatory Technical Standard that can supplement the specifications of eIDAS.[772] In one case, it was supported that in an ideal situation unlinkability should be supported, on top of selective disclosure and pseudonymisation, by anonymous credentials. With anonymous credentials, the eIDAS nodes would be able to transmit assertions that do not disclose any personal data, for example by verifying the legal age through a computation of the current age of the user rather than the disclosure of their date of birth.[773] Although building in such functionality would only require a common trust list – which FutureTrust is building in its Global Trust List, and a common definition of the national identifiers – which again is in large served through the FutureTrust eID module,[774] it was pointed out that deployment at an EU scale could have a performance impact,[775] therefore selective disclosure and pseudonymisation might be preferable. An exception to the above was the case of the UK expert who felt that the number of identifiers present in the Minimum Dataset is the minimum required for most transactions[776] and, in any case, can be

[769] *"data minimisation and selective disclosure, they can be through the STORK framework. So they can review information that you can share and all of that. So I believe that's working there."* appendix B lines 1710–1712; *"Technically no problem. It would work. It is just for the initial deployment, and as we do not yet know what other member states make as conditions for private sector use."* appendix B lines 471–473; *"this is probably the pragmatic way out, that the eIDAS nodes are trustworthy and they are trusted to take care that the privacy regulation which are, when eIDAS started there were different regulations, but by now they are harmonised and if there's an eID scheme which is not yet privacy friendly the eIDAS nodes, yeah, should be oblige to take care that this doesn't hurt in the end."* appendix B lines 1551–1556.

[770] *"I mean that was discussed in, that was discussed in the council and also in the expert [unclear] technical subgroup. And the compromise given that, for instance, some member states do not have the system identifiers, or have several identifiers."* appendix B lines 224–227; *"In the technical subgroup, we are discussing the possibility that to amend the specification in a way that if a service doesn't request the minimum data set, that you just can deliver the first name, for instance, and things like that. But the current specification refrained from that, and I strongly supported that. In particular to make sure that the initial deployment was, yes, this works."* appendix B lines 237–242.

[771] *"That's why we in Austria decided to go for sector specific identifiers. [...] So we would love other member states to do that similarly."* appendix B lines 207–212.

[772] *"they publish things that they call RTS, is a regulatory technical standards which define the technical stuff under the regulation. And there, they can prescribe protocols and things like data."* appendix B lines 825–827.

[773] *"so explore the idea of not releasing, for example, the birth date if you are buying alcohol. Just answering if the person is over 18 or not."* appendix B lines 1702–1704.

[774] *"what we'd require is a common definition on the formats of the information that is so on the credentials, that can be exchanged and a trust on the certification authority, so a trust list."* appendix B lines 1778–1780.

[775] *"My view on anonymous credentials is that, well, it is rather complex and there are some performance impact at least from previous experience"* appendix B lines 1747–1748.

[776] *"given it's only three items it's pretty minimal"* appendix B line 1840; *"the number of services that would not want to, for example, personalise it by your first name is fairly limited realistically in a competitive marketplace at the moment with current privacy attitudes."* appendix B lines 1863–1866.

justified against the costs, effort and computational overhead that selective disclosure and pseudonymisation would add to the infrastructure.[777]

9.4 Conclusion

On the whole, the expert data supports the relevance of the analysis of the state of the art in the field of eID as deployed within chapter 8. The experts agree that unlinkability is a key goal against the risks that unique identifiers pose. Notable, there are cases where the presence of unique identifiers are not perceived as risky (Estonia) or cases where it is considered that the overhead to produce pseudonymous credentials would not be justified by the risk (the UK). In the former case, this attitude has to do with the approach taken in Estonia that certain personal data, like the unique identifier, name and data of birth, are public data and should be used freely. In the latter case, the risk of re-use is recognised, but the existence of a unique identifier of some permanence along with the name and date of birth are considered as the minimum necessary data for the needs of public-sector bodies. However, in both cases the attitudes expressed concern the circulation of that data within the territory of the issuing Member State, not the cross-border authentication that would happen under eIDAS.

In any case, the need for strong technical control was repeatedly highlighted. Soft measures that rely on policies, although still used by some Member States, are not regarded as suitable in a cross-border environment, because of a lack of enforcement options. It was recognised that for schemes that rely on technical controls for unlinkability, participation within the Interoperability Framework as it currently stands will most likely lead to weaker unlinkability protections.

And, although this was seen as a necessary compromise for the needs of the public-sector by some, at large it was agreed that if private-sector services start relying on the Interoperability Framework stronger technical measures would be needed. This was mainly due to the belief that the private-sector has less reliability than the public-sector in terms of re-using personal data for other purposes.

Finally, a possibility to introduce stronger unlinkability through selective disclosure and pseudonymisation was met with approval, with the majority of experts agreeing that it would offer a significant improvement. The dissenting opinion argued against pseudonymisation and selective disclosure because of a concern about the cost and effort of implementation.

[777] *"Doing it differently actually increases certain risks and a... Both increases certain risks and increases the complexity of the code. And increased complexity of code introduces additional risks as well. So this is not an unreasonable approach to take."* appendix B lines 2265–2267.

Given this endorsement of the analysis that has been presented, the next chapter discusses the implications of the current limitations of the Interoperability Framework and formulates a recommendation to extend the level of unlinkability supported.

Chapter 10

Reinforcing unlinkability in the Interoperability Framework

...the controller shall [...] implement appropriate technical and organisational measures [...] in an effective manner
— GDPR Art 25(1)

10.1 Introduction

In chapter 5 it was argued that eID is considered as processing likely to result in high-risks by some national DPAs. Regardless of its characterisation, however, the threshold analysis in chapter 6 has demonstrated that pseudonymisation and selective disclosure are key measures of unlinkability, one of the seven goals of data protection by design. Chapter 7 examined the unlinkability afforded by the Interoperability Framework and found that the goal is only partially met under the current specifications. It was argued in chapter 7 that, regardless of the likelihood of high-risks, eIDAS will lower the level of unlinkability that can be achieved on national schemes that depend on high levels of unlinkability. Lowering the level of data protection by design of the national eID schemes can only be considered in compliance with the Article 25 GDPR if justified against the state of the art and the cost of implementation. An examination of the state of the art in chapter 8 has revealed that there are different levels of unlinkability among national eID schemes: the highest level can be observed in Germany's nPA which is equipped with full selective disclosure and pseudonymisation capabilities. However, the bare minimum level across the eID schemes examined was the substitution of permanent unique identifiers with sector-specific identifiers, through the use of pseudonymous (i.e. nonsensical) attributes. The importance of the goal of unlinkability, the key role pseudonymisation and selective disclosure play in it, as well as the effect that participation in eIDAS will have for national eID schemes, was evaluated by the expert data in chapter 9.

This chapter discusses the assumptions of the current implementation of unlinkability in eIDAS. It argues that when considering a bigger picture where eIDAS is embraced not only by the public-sector but also by private online services, as indeed the aspiration of the drafters of eIDAS seems to be, the current level of unlinkability will not be adequate. The state of the art, the nature, scope, context and purposes of processing and the risks for the rights and freedoms of individuals cannot justify the effect of weakening unlinkability for eID schemes just by virtue of participation in the Interoperability Framework.

The last criterion of Article 25, the cost of implementation, is subsequently further discussed. It is proposed that unlinkability support can be improved in eIDAS by an extension of the SAML protocols that are used for communication between the eID schemes and the services. Such a solution is a practical way out to allow national eID schemes participation in eIDAS without sacrificing the levels of unlinkability they support. A cost-effective way to implement the SAML extension is proposed.

Section 10.2 recaps the shortcomings of the Interoperability Framework in terms of unlinkability and further discusses the implications for the level of data protection by design afforded by the Interoperability Framework. A practical solution to align the level of unlinkability, and hence the level of data protection by design, afforded by the Interoperability Framework with the levels of the participating eID schemes is presented in section 10.3. Of note, part of the material presented in this chapter has been used in *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness*[778] and published under *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*[779]

10.2 Addressing the Shortcomings of Unlinkability in the Interoperability Framework

As was explained in section 6.2, the data protection goal of unlinkability comprises measures to effect data minimisation and purpose limitation. Unlinkability controls and mitigates the ability to aggregate data that could identify or profile an individual. As was shown in chapter 8, national implementations of eID effect unlinkability through the use of two techniques: The substitution of identifying information with pseudonyms

[778] Niko Tsakalakis and Sophie Stalla-Bourdillon, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

[779] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'Hara, *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"* in Eleni Kosta and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Eleni Kosta and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

and the controlled disclosure of only absolutely necessary attributes for the purpose through selective disclosure. These techniques should be regarded as part of the state of the art, which was confirmed by the experts' opinions.[780] The measures, which coincide with the controls provided as examples by GDPR Article 25, satisfy the definition of pseudonymisation under the GDPR when adopted jointly.

The Interoperability Framework attempts to satisfy data minimisation through alternative measures that, however, fall short of having the same effect as the state of the art. Although in principle eIDAS enforces data minimisation through a strict definition of transmitted attributes that form the Minimum Dataset, this approach falls short for two reasons:

- Firstly, because of the existence of the Minimum Dataset. The rationale behind the existence of a Minimum Dataset is the assumption that all electronic services participating in the Interoperability Framework require at least the mandatory attributes of the Minimum Dataset to correctly accomplish their purpose.
- Secondly, because of the impact of the Minimum Dataset on effective pseudonymisation. As is the intention of eIDAS, the mandatory attributes of the Minimum Dataset – whether the unique identifier is of the form of a pseudonym or not – are enough to uniquely identify an individual. Since effective pseudonymisation can only exist when other accompanying attributes contain no identifying information,[781] the presence of a mandatory set of attributes in every transaction and the inclusion of a persistent unique identifier automatically precludes any meaningful use of selective disclosure and pseudonymisation.

The assumed necessity of both reasons is examined below.

The working assumption that the Minimum Dataset would be necessary in any case is only *prima facie* correct. Indeed, when one considers as eIDAS' subject matter only the citizen-facing e-government service it would seem that a person's full name and date of birth would be necessary to effectively differentiate between citizens. However, this is wrong. For one, eIDAS automatically applies to all *"public sector bod[ies]"*,[782] This definition encompasses a plethora of services, with purposes and needs that differ from Member State to Member State. Some of the services only require the ability to uniquely identify a person upon first use of the service. In subsequent uses, a connection to a form of identifier created by the service is enough to ensure continuity of service (for

[780] nn 747 and 748 and related text.

[781] See section 7.2.

[782] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73, art 3(7): *"'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;"*.

example, to ensure that the actions of the person will be saved under the correct record). In other words, electronic identification is required only the first time; subsequent uses only require adequate authentication which can be satisfied without the existence of identifying attributes. Although eIDAS (implicitly) recognises this difference in the definition of authentication,[783] it provides no mechanism to effect it.

Some Member States already offer a high level of unlinkability. Yet, the Interoperability Framework seems to be quite restrictive when it comes to implementing the goal of unlinkability, because of the presence of the Minimum Dataset and the inherent limitations it puts to pseudonymisation. As a result, national schemes that support a high level of unlinkability will still be able to guarantee such a level for cross-border transactions. Importantly, because acceptance of eID schemes of a LoA 'Substantial' or 'High' is mandatory, Member States with a high degree of unlinkability will not be in a position to refuse to connect their schemes to national eID schemes of a lower degree of unlinkability. As a result, there is an argument that eIDAS Article 12(3)(c) would not be met in the sense that the Interoperability Framework would undermine rather than facilitate privacy by design. Going further, national data controllers enabling and operating eID and authentication cross-border would be prevented from offering to their users a high level of data protection. This could have implications in terms of liability as eIDAS Article 11 should be combined with the compensation of GDPR Article 82 (and eventually the administrative fines of Article 83).

Evidently, a level of unlinkability that results in a decrease of the level of data protection by design that a national scheme offers is inadequate. Limiting the unlinkability controls of national schemes raises questions as to how the Interoperability Framework can claim to satisfy eIDAS Article 12(3)(c) obligation to facilitate privacy by design. Most importantly, it was shown that the nature of processing for the purposes of eID has already been considered as likely to result in high-risk by some national DPAs which would warrant increased protection measures. And, it was demonstrated that the state of the art has evolved towards sector-specific identifiers and selective disclosure. It is doubtful, therefore, under the limitations of the Interoperability Framework that data protection by design is complied with.

Further, as shown during past cross-border pilots[784] but also emerged from the expert data analysis,[785] there are public-sector services that require less information than the mandatory part of the Minimum Dataset. In fact, services like the anonymous chat that was piloted during the STORK 2.0 project would not be possible under eIDAS' Minimum Dataset. Besides, eIDAS has already shown an aspiration to extend its application

[783] eIDAS (n 782) art 3(5): *"'authentication' means an electronic process that enables the electronic identification of a natural or legal person,* ***or the origin and integrity of data in electronic form to be confirmed;"*** [emphasis given].

[784] See Thomas Knall and others, *"Secure and Privacy-Preserving Cross-Border Authentication: The STORK Pilot 'SaferChat'"* (Kim Normann Andersen and others eds, Springer Berlin Heidelberg 2011).

[785] See nn 759, 760 and 766 and related text.

beyond public-sector services.[786] Private services, in contrast to e-government services, rarely require to uniquely identify an individual to provide an effective service.[787] Taking as an example the biggest online social platforms, Facebook and Twitter, a username and password suffices for them to be able to provide their services. Notably, Facebook applies a *"real-name policy"*[788] which however is not enforced by default and its goal is not to identify the users but instead ensure that users *"[u]se the same name that [they] use in everyday life."*[789] Twitter, on the other hand, does not regulate whether users use their real names or pseudonyms.[790] Moreover, because of the private nature of those services and the variability of their purposes, use of a Minimum Dataset as a 'one-size-fits-all' is regarded as excessive.[791] The view is accompanied with a distrust as to how private companies can or would use such datasets.[792]

An extension of eIDAS' applicability to private sector services should prompt a discussion on how to improve unlinkability within the Interoperability Framework. Yet, the mere fact that participating national schemes possess a higher level of unlinkability which are prevented from using, indicates that the way the Interoperability Framework addresses unlinkability should be improved even when talking about public sector services. Besides, as shown in the previous paragraphs there is a strong argument that the current data minimisation measures would fail the appropriateness test considering the contextual factors of the nature and purposes of the processing, the risks of non-implementation and the state of the art.

The last contextual factor of GDPR Article 25, the cost of implementation is addressed below. The following section presents a potential solution that can support a level of unlinkability equivalent to the one of the participating national schemes. The solution constitutes a practical way out with minimal cost, both in terms of monetary costs and in terms of implementation costs.

10.3 Extending the Support of Pseudonymisation and Selective Disclosure

In order to guarantee a level of data protection by design within the Interoperability Framework that is equivalent of the levels that the sum of the national schemes provide,

[786] See n 36.

[787] n 765 and related text.

[788] *"Facebook's Name Policy"* (*Facebook*, 2019) ⟨https://www.facebook.com/help/292517374180078⟩ accessed 10 September 2019 (archived at ⟨https://archive.fo/CEq7X⟩).

[789] *"Terms of Service"* (*Facebook*, 2019) ⟨https://www.facebook.com/legal/terms/plain_text_terms⟩ accessed 17 September 2019 (archived at ⟨http://archive.fo/mS3Rr⟩) 3(1).

[790] Mathew Ingram, *"Why Twitter doesn't care what your real name is" GigaOM Technology Blog* (Austin, TX, 16 September 2011) ⟨https://gigaom.com/2011/09/16/why-twitter-doesnt-care-what-your-real-name-is/⟩ accessed 2 September 2019 (archived at ⟨http://archive.fo/ZZOiD⟩) .

[791] nn 761, 763 and 764 and related text.

[792] n 762 and related text.

better facilitation of selective disclosure and pseudonymisation is needed. Support for selective disclosure and pseudonymisation will allow those national eID schemes that support them to operate within the Interoperability Framework under the same data protection guarantees they offer in domestic eID.

As aforementioned, the restrictions placed upon selective disclosure and pseudonymisation are the result of the Minimum Dataset, its mandatory attributes and its unique identifier. However, the Minimum Dataset ensures that disparate national eID schemes have a common denominator that is necessary for them to interoperate. Besides, the Minimum Dataset is already prescribed by the text of eIDAS and its implementing regulations.

A way to increase the degree of unlinkability in eIDAS would be through the data privacy design strategies *"MINIMISE"*, *"HIDE"*, *"SEPARATE"* and *"AGGREGATE"*.[793] The four strategies aim to effect unlinkability by processing only the minimum amount of data possible and by restricting the information contained within through aggregation and masking so that two events in the system[794] cannot be related to one another. The use of pseudonyms, if combined with selective disclosure, can implement these strategies.[795] The Interoperability Framework can be modified to accommodate selective disclosure and pseudonymisation. It is true that modifying the Framework to accept different capabilities depending on the affordances of the national scheme might be impossible, as it would require an upfront insight into the design of all EU schemes – whose notification under the Framework is after all voluntary and, hence, not guaranteed.

Any attempt to increase support of selective disclosure and pseudonymisation cannot disregard the (limited) specifications of eIDAS. For successful support, therefore, a solution is needed that (a) conforms to eIDAS and its requirements about the Interoperability Framework, (b) provides a way to implement selective disclosure and pseudonymisation for these national schemes that support them, and (c) is relatively easy to execute optimally without modification of eIDAS or its implementing acts.

A potential answer that satisfies these conditions could be through an extension of the supported SAML exchanges[796] so that the eIDAS nodes, rather than the national schemes or the Interoperability Framework, would be altered.

[793] As recommended by ENISA: George Danezis and others, *Privacy and Data Protection by Design – from policy to engineering* (ENISA report, 2014) DOI: 10.2824/38623 18-20.

[794] *"where events can be understood to include data subjects doing something, as well as data items that occur as the result of an event"*: ibid 19.

[795] Use of pseudonyms is proposed as a *"design pattern"* for the *"MINIMISE"* and *"HIDE"* strategies, whereas selective disclosure can assist in *"AGGREGATE"* and *"SEPARATE"* when used in a federated system: ibid 19-20.

[796] The national systems, the deployed eIDAS nodes and the Service Providers communicate through defined queries and answers in Security Assertion Markup Language (SAML). See eIDAS Technical Sub-group, *eIDAS SAML Attribute Profile* (v. 1.1.2, 2016) ⟨https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf⟩ accessed 4 November 2016 (archived at ⟨http://archive.fo/pLWy5⟩).

Under the current SAML profile, schemes interfacing with eIDAS *"MUST support at least all mandatory attributes"*.[797] When an authentication request is performed, attributes that belong to the mandatory part of the Minimum Dataset are flagged with an attribute ⟨`isRequired`⟩ set to `true`. Optional attributes from the Minimum Dataset *"MAY"* be requested,[798] and additional attributes *"MAY"* be supported after agreement between the parties.[799] However, currently *"[w]hen requesting a minimum dataset, at least all attributes defined as mandatory within this minimum data set MUST be requested."* (listing 10.1)[800]

As for the unique identifier, under the same specifications it *"shall remain unchanged for the lifetime of the account"*.[801] This condition has not always been interpreted strictly, with the eIDAS Cooperation Network opining that *"lifelong-peristen[ce]" "is not a requirement under the eIDAS regulation."*[802] The format of the identifier is up to the national scheme. However, for schemes that operate with sector-specific identifiers[803] it is up to the discrethion of the Member State to implement additional arrangements.[804] Evidently, the power lies with the receiving Member State; i.e. Austria will be able to construct sector-specific identifiers out of the received Minimum Dataset's identifier to make them compatible with its national scheme, but it has no power to demand other Member States to accept its sector-specific identifiers.

[797] eIDAS Technical Sub-group, *eIDAS SAML Message Format* (v 1.1.2, 2016) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_message_format_v1.0.pdf?version=1&modificationDate=1497252920416&api=v2⟩ accessed 4 November 2019 (archived at ⟨https://tinyurl.com/y6u2qnds⟩) para 2.3.1: *"eIDAS-Services MUST support at least all mandatory attributes as specified in [eIDAS-Attr-Profile]. Optional attributes of [eIDAS-Attr-Profile]SHOULD be supported."*

[798] ibid para 2.3.2.

[799] ibid para 2.3.1.

[800] ibid para 2.3.2.

[801] eIDAS Technical Sub-group, *eIDAS SAML Attribute Profile* (n 796) 23.

[802] Freek van Krevel, *PEER REVIEW REPORT – German eID* (DG Connect, Digital Single Market, eIDAS Cooperation Network, v 1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/Peer%20review%20report%20German%20eID%20-%2016062017.pdf?version=1&modificationDate=1499172190851&api=v2⟩ accessed 23 July 2019 (archived at ⟨http://archive.fo/3I24w⟩) 18; note that in the case of the German notification, the expiration of a person's ID card (whose lifetime is 10 years) and the issuance of a new ID card was interpreted as the end of the lifetime of the account and, therefore, issuance of a new unique identifier (i.e. a pairwise-persistent pseudonym) is permitted: ibid 18.

[803] See e.g. the Austrian, German and UK schemes in chapter 8.

[804] *" Where additional sector specific attributes are required Member States and domain experts are invited to develop additional attribute schema describing the type and usage of these attributes for inclusion in Member State eIDAS Node metadata."* (eIDAS Technical Sub-group, *eIDAS SAML Attribute Profile* [n 796] 23).

```
<saml2p:Extensions>
  <eidas:SPType>public</eidas:SPType>
  <eidas:RequestedAttributes>
    <eidas:RequestedAttribute Name=”http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier”
      NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname−format:uri” isRequired=”true”/>
    <eidas:RequestedAttribute Name=”http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName”
      NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname−format:uri” isRequired=”true”/>
    <eidas:RequestedAttribute Name=”http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName”
      NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname−format:uri” isRequired=”true”/>
    <eidas:RequestedAttribute Name=”http://eidas.europa.eu/attributes/naturalperson/DateOfBirth”
      NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname−format:uri” isRequired=”true”/>
  </eidas:RequestedAttributes>
</saml2p:Extensions>
```

Listing 10.1: eIDAS SAML Authentication Request[805]

Regardless, it is the flexibility on the implementation of the received unique identifier that can provide a practical way out of the constrains put on pseudonymisation, coupled with an alteration to the way selective disclosure is handled. The SAML exchanges could be modified to distinguish and accept requests for a smaller number of identifiers than the ones present in the Minimum Dataset. The number of requested identifiers would depend on the requirements of the Service Provider.

eIDAS defined the content of the Minimum Dataset on the assumption that all public-sector services would require the mandatory attributes to be able to successfully authenticate an individual. It is arguable whether this assumption holds true for all public-sector services.[806] For example, the STORK project had piloted a public-sector anonymous online chat room service, aimed at teenagers, which accepted only attributes of age.[807] Contrary opinions were also expressed during the expert interviews.[808] Besides, the decision for a unique identifier has already forced some Member States to alter how the eIDAS-nodes will work in their territory.[809] Even working under the assumption that the mandatory attributes are essential for public-sector services, the same does not – and should not – hold true for the private sector, to where eIDAS aspires to expand. In any case, therefore, incorporation of selective disclosure and pseudonymisation into the Interoperability Framework will prove valuable.

Of note, the STORK 2.0 project, which formed the basis for the eIDAS Interoperability Framework, defined a SAML profile capable of selective disclosure (listing 10.2). All attributes requested under STORK 2.0 could be flagged as optional, and, thus, could be omitted from transmission without necessarily resulting in a failed authentication.[810]

[805] eIDAS Technical Sub-group, *eIDAS SAML Attribute Profile* (n 796).

[806] See text of nn 782 and 783.

[807] Knall and others (n 784) 104.

[808] See text of nn 759 and 761.

[809] See n 749.

[810] STORK, *Final Version of Technical Specifications for the cross-border interface: Secure idenTity acrOss boRders linKed 2.0 – STORK 2.0* (D4.11, 2015) ⟨https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174⟩ accessed 3 August 2018 23.

```
<complexType name=”RequestedAttributeType”>
  <sequence>
    <element ref=”stork:AttributeValue” type=”anyType” minOccurs=”0” maxOccurs=”unbounded”/>
  </sequence>
  <attribute name=”Name” type=”string” use=”required”/>
  <attribute name=”NameFormat” type=”anyURI” use=”required”/>
  <attribute name=”FriendlyName” type=”string” use=”optional”/>
  <anyAttribute namespace=”##other” processContents=”lax”/>
  <attribute name=”isRequired” type=”boolean” use=”optional”/>
</complexType>
```

Listing 10.2: STORK 2.0 Requested Attribute[811]

The SAML profile that regulates the communication between the eIDAS nodes could be extended to support such functionality, in a similar fashion to the extension by Horsch, Tuengerthal, and Wich – which is proposed however as a solution to a different scenario of Web Browser SSO.[812] An extension of the eIDAS SAML profile would permit Service Providers to specify necessary attributes to their `AuthnRequest`. The `AuthnRequest` would, therefore, be remodelled according to listing 10.3, lines 21–26, to include a ⟨`RequestedAttributeInfo`⟩ element. The requested attributes would be described in the element, with a `"required"` or `"optional"` flag, to signify whether an attribute is essential or not.

```
 1 <md:SPSSODescriptor protocolSupportEnumeration=”urn:oasis:names:tc:SAML:2.0:protocol”>
 2   <md:Extensions>
 3     <mdui:UIInfo>
 4       <mdui:DisplayName xml:lang=”en”>SP1</mdui:DisplayName>
 5       <mdui:Description xml:lang=”en”>Description.</mdui:Description>
 6       <pe:RequestedAttributeInfo AttributeName=”urn:oid:2.5.4.42”>
 7         <pe:Purpose xml:lang=”en”>To call you.</pe:Purpose>
 8       </pe:RequestedAttributeInfo>
 9       <pe:RequestedAttributeInfo AttributeName=”urn:oid:2.5.4.41”>
10         <pe:Purpose xml:lang=”en”>Enhanced user experience.</pe:Purpose>
11       </pe:RequestedAttributeInfo>
12     </mdui:UIInfo>
13   </md:Extensions>
14   <md:AssertionConsumerService index=”0” isDefault=”true” Location=”https://sp1.example.com/saml” Binding=”urn:oasis:
         ↪ names:tc:SAML:2.0:bindings:HTTP−POST”>
15   </md:AssertionConsumerService>
16   <md:AttributeConsumingService index=”0” isDefault=”true”>
17     <md:ServiceName xml:lang=”en”>SP1</md:ServiceName>
18     <md:RequestedAttribute Name=”urn:oid:2.5.4.42” isRequired=”true” FriendlyName=”Forename” NameFormat=”urn:oasis:
         ↪ names:tc:SAML:2.0:attrname−format:uri”> </md:RequestedAttribute>
19     <md:RequestedAttribute Name=”urn:oid:2.5.4.41” isRequired=”false” FriendlyName=”Name” NameFormat=”urn:oasis:
         ↪ names:tc:SAML:2.0:attrname−format:uri”> </md:RequestedAttribute>
20   </md:AttributeConsumingService>
21   <element name=”RequestedAttributeInfo”>
22     <complexType>
23       <attribute name=”urn:oid:2.5.4.42” type=”string” use=”required” />
24       <attribute name=”urn:oid:2.5.4.41” type=”string” use=”optional” />
25     </complexType>
26   </element>
27 </md:SPSSODescriptor>
```

Listing 10.3: SAML Privacy-Enhancing Profile[813]

[811] ibid 22.

[812] Moritz Horsch, Max Tuengerthal, and Tobias Wich, *“SAML Privacy-Enhancing Profile”* (Detlef Hühnlein and Heiko Roßnagel eds, Stuttgart, Germany, Gesellschaft für Informatik eV 2014) 19–20.

[813] As adapted for the purposes of the Interoperability Framework from ibid 16–17.

Importantly, the extension can be set to apply only to the communication between the eIDAS node (i.e. of the receiving Member State) and the Service Provider(s). This will allow for the communication between the sending and the receiving Member States to operate under the current SAML profile, permitting the transmission of the Minimum Dataset in its entirety and, thus, maintain conformance to the eIDAS requirements.

The sending Member State would send the Minimum Dataset, containing at least the mandatory attributes. This would ensure that (receiving) Member States with national schemes that do not natively support selective disclosure and pseudonymisation would still be able to receive authentication attestations. The eIDAS node, having received the Minimum Dataset, would then be able to intercept which of the attributes are necessary for the purposes of the Service Provider and repackage the Minimum Dataset into a dataset that includes only the `"required"` attributes, as per figure 10.1.[814] During the repackaging, the eIDAS node will be able to substitute the unique identifier received as part of the Minimum Dataset with a pseudonym generated on the fly specifically for the requesting Service Provider. Under circumstances where the `"required"` attributes are non-identifying (e.g. a date of birth), this process will produce a fully pseudonymised dataset in the meaning of GDPR Article 4(5).

A comparable architecture was proposed for the needs of the EU-funded project 'FutureID', which designed a federated system for cross-border eID. The FutureID broker in the federation could act in a *"claims transformer mode"* and transform the authentication claim to SAML session credentials or attribute-based credentials.[815] However, in contrast to the FutureID broker, in the proposed solution here the eIDAS node will not perform the authentication itself. It will instead receive the Minimum Dataset as transmitted by the scheme that performed the authentication and repackage it for transmission to the Service Provider.

An implementation at the level of the eIDAS node can counterbalance the necessary concessions that national schemes with advanced privacy features (i.e. sector specific identifiers, selective disclosure) would have had to make to participate in the Interoperability Framework. Although the method of deployment of the eIDAS nodes will impact the effectiveness of selective disclosure and pseudonymisation, the solution will provide benefits regardless of method.

Four deployment methods can be distinguished (depicted in figure 10.2):

i. Centralised deployments:

[814] A similar re-packaging is performed in systems with a hub-and-spoke architecture. See the data flow of Gov.UK Verify in Niko Tsakalakis, Kieron O'Hara, and Sophie Stalla-Bourdillon, *"Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation"* (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), 21 May 2016, Hannover, Germany, 2016) DOI: 10.1145/2908131.2908152.

[815] Heiko Roßnagel and others, *"FutureID – Shaping the Future of Electronic Identity"* (Limassol, Cyprus, Annual Privacy Forum 2012, 10–11 October 2012, 2012) s 3.2.

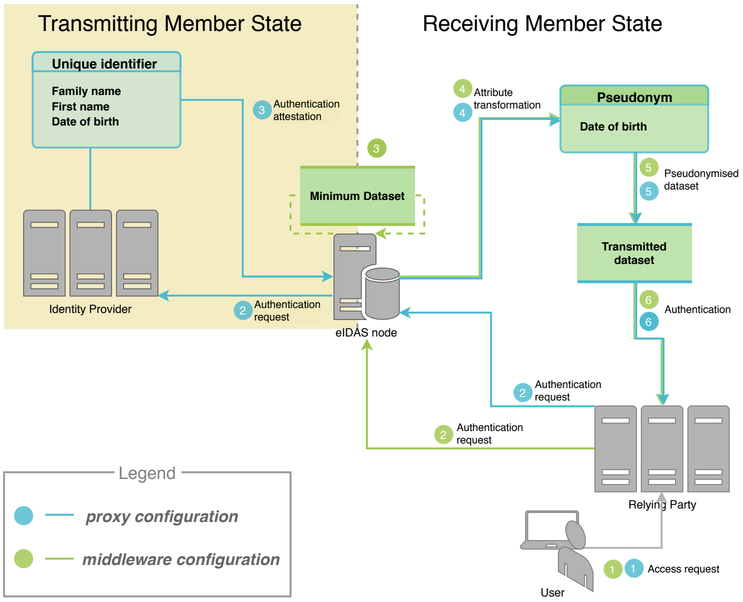


FIGURE 10.1: eIDAS node with selective disclosure and pseudonymisation capabilities

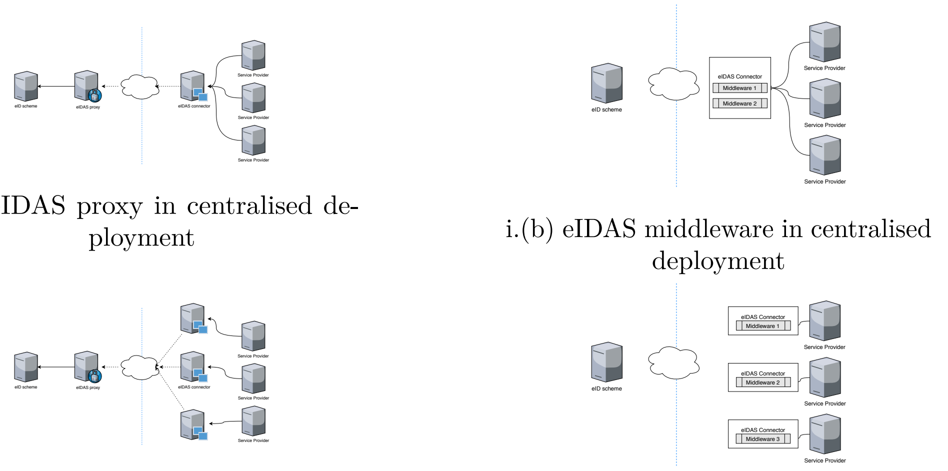
(a) The sending Member State operates an eIDAS node as a proxy service. The receiving Member State operates an eIDAS node as an 'eIDAS-Connector'. Service Providers send authentication requests through the same eIDAS Connector to the eIDAS proxy, who relays the requests and the authentication assertions to the notified eID scheme.

(b) The sending Member State provides a middleware to the receiving Member State. The middleware is operated by the receiving Member State. The receiving Member State operates an eIDAS node as an 'eIDAS-Connector', which incorporates the middleware. Service Providers send authentication requests to the eIDAS Connector. Authentication is performed by the middleware.

ii. Decentralised deployments:

(a) The sending Member State operates an eIDAS node as a proxy service. The receiving Member State operates several eIDAS nodes as eIDAS-Connectors. Service Providers send authentication requests through different eIDAS Connectors to the eIDAS proxy, who relays the requests and the authentication assertions to the notified eID scheme.

(b) The sending Member State provides several instances of middleware to the receiving Member State, which will be operated by the receiving Member State. Each eIDAS Connector at the receiving Member State incorporates an instance of the middleware. Service Providers connect to different eIDAS Connectors, where authentication is performed locally.



i.(a) eIDAS proxy in centralised deployment

i.(b) eIDAS middleware in centralised deployment

ii.(a) eIDAS proxy in decentralised deployment

ii.(b) eIDAS middleware in decentralised deployment

FIGURE 10.2: Possible configurations between sending and receiving Member States[816]

Introducing unlinkability to the eIDAS node would have different effects for the individual configurations in terms of the disclosed attributes and the unique identifier:

Deployment i.(a): When Service Providers request authentications under the same eIDAS Connector, introducing unlinkability capabilities will allow the Connector to selectively disclose these attributes that are absolutely necessary for each authentication. The Connector will also be able to construct pseudonyms to replace the unique identifier received by the eIDAS proxy. However, because the Connector is always the same, the Minimum Datasets that it will be receiving will have to always be the same as well (i.e. the eIDAS proxy will not be able to substitute the unique identifier, or any substitution will be meaningless since it will be accompanied by the rest of the attributes of the Minimum Dataset).

Deployment i.(b): A similar effect will take place when the sending Member State opts for a centralised middleware configuration. The difference is that since authentication happens locally at the middleware level, there is no transmission of personal data between the sending and receiving Member States.

Deployment ii.(a): In authentications against an eIDAS Proxy, but where the Service Providers connect to different eIDAS Connectors, the added benefit it that pseudonymisation can happen also at the Proxy level. This would function similarly to the hub-and-spoke federation models, allowing the eIDAS proxy to substitute the unique identifier with a pseudonym. Consequently, the unique identifier of the

[816] As adapted from eIDAS Technical Sub-group, *eIDAS – Interoperability Architecture* (v1.00, 2015) ⟨https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/82797006/eidas_interoperability_architecture_v1.00.pdf⟩ accessed 22 June 2019 (archived at ⟨https://tinyurl.com/vmao3rp⟩) 3–4.

Minimum Dataset would not have to be transmitted at all, i.e. introducing an extra measure of unlinkability.

Deployment ii.(b): Finally, where Service Providers connect to different eIDAS Connectors operating different instances of middleware, the unlinkability that can be achieved through the selection of attributes and the pseudonymisation of the unique identifier is greater. This is because multiple instances of the middleware will ensure that the pairwise-persistent pseudonyms created will be entirely different per Service Provider (i.e. both components of the pair Middleware $\longleftrightarrow$ Service Provider will differ), hence mitigating risks of (malicious) Service Providers being able to use the same middleware to aggregate datasets.

In all cases, Service Providers will be receiving only a subset of identifiers suitable to their needs, which effectively reduces the risk of data collusion either at the Service Provider level or during transit from the node to the Service Provider. Such an amendment offers advantages, even under the assumption that public-sector services will indeed need all attributes of the Minimum Dataset to perform matching correctly.[817] Considering the private-sector, the Minimum Dataset will be over-abundant for many services, for example for the needs of online social platforms. Further, private-sector services operate under different obligations and potentially less scrutiny.[818] Instead of treating necessary attributes as a 'one-size-fits-all', therefore, it would make better sense to adjust the transmitted attributes on a case-by-case basis.

Additionally, implementation of this solution at an EU level would benefit unlinkability. In principle, no constraints are in place and Member States are free to implement an eIDAS node that goes beyond the current specifications and supports additional unlinkability functionality. However, the decision of implementation is at the discretion of the receiving Member State. This creates a power imbalance that places the sending Member State in a difficult position, since – if the sending Member State supports selective disclosure and pseudonymisation – it has no power to enforce their support by the receiving Member State. A design that incorporates this solution into the eIDAS node architecture can be agreed at an EU level, without the need for complex time-consuming procedures.

[817] Although, as it has been already pointed out, this is not a reasonable assumption. See text of nn 806 and 808.

[818] For example, it is easier for them to on consent or legitimate interests as their legal basis and the obligation to appoint a DPO does not always apply to the private sector. See ICO, *Guide to the General Data Protection Regulation* (1,0,154, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf⟩ accessed 24 May 2018 (archived at ⟨https://tinyurl.com/y9pr9o2x⟩) 60,80,205.

Instead, the design of the eIDAS nodes can be modified through an Implementing Act or a Regulatory Technical Standard (RTS).[819] Impl Reg 2015/1501 allows for discretion in modifying or expanding the technical specifications, under the procedure of Article 12.[820] Further, modification of the SAML profile is possible if it is *"based on standards that have already been deployed more than once between Member States and proven to work in an operational environment."*[821] Both conditions can easily be proven, as shown in the aforementioned analysis. An RTS can be agreed by the eIDAS Cooperation Network, where the extension of the SAML profile is added to the current specifications about the eIDAS nodes. Implementation via an RTS ensures uniform applicability, while being non-intrusive in terms of the level of abstraction needed in order to remain technology-neutral. Further, it provides a simple and quick way to address unlinkability without a need to amend eIDAS or its Implementing Acts and without introducing further financial obligations. In other words, it presents an opportunity for data controllers in the field of eID to align with the state-of-the-art to address the risks to the rights and freedoms of the data subjects, in line with the nature, scope, context and purposes of processing and without disproportionate cost of implementation.

Selective disclosure and pseudonymisation, implemented in this way would therefore ensure a greater level of data minimisation and unlinkability, facilitating the implementation of the data protection principles of data minimisation and purpose limitation and thereby the principle of data protection by design for cross-border transactions without compromising the levels of data minimisation and unlinkability set domestically within each national eID scheme. This would be in line with the view that the GDPR

[819] RTSs are delegated acts of a technical nature, prepared by an EU Supervisory Authority. Their goal is to *"further develop, specify and determine the conditions for consistent harmonisation of the rules included in the basic legislative act."* (Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014 amending Directives 2003/71/EC and 2009/138/EC and Regulations (EC) No 1060/2009, (EU) No 1094/2010 and (EU) No 1095/2010 in respect of the powers of the European Supervisory Authority (European Insurance and Occupational Pensions Authority) and the European Supervisory Authority (European Securities and Markets Authority) [2014] OJ L153/1, rec 11; European Commission, *"Powers of the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority ***I Proposal for a directive of the European Parliament and of the Council amending Directives 98/26/EC, 2002/87/EC, 2003/6/EC, 2003/41/EC, 2003/71/EC, 2004/39/EC, 2004/109/EC, 2005/60/EC, 2006/48/EC, 2006/49/EC, and 2009/65/EC in respect of the powers of the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority"* COM(2009)0576 – C7-0251/2009 – 2009/0161(COD), rec 9) Their advantage to Implementing Acts is that the legislative procedure to adopt an RTS is shorter (this advantage is, for example, being used by the Commission in its legislative response to the COVID-19 pandemic. See European Commission, *"Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) No 575/2013 and (EU) 2019/876 as regards adjustments in response to the COVID-19 pandemic"* COM(2020) 310 final, 8).

[820] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1, art 12(1): *"the Cooperation Network established by Implementing Decision (EU) 2015/296 may adopt opinions pursuant to Article 14(d) thereof on the need to develop technical specifications. Such technical specifications shall provide further details on technical requirements as set out in this Regulation."*

[821] ibid art 8.

mandates "custom built" approaches[822] that depend on the facts and circumstances of each particular processing. However, it would make it possible to prevent the erosion of a high level of data protection when participating in cross-border eID and to mitigate the downsides of interoperability and mutual recognition. Importantly, the proposition of such an implementation found the experts, generally, in agreement.

10.3.1 Conclusion

Unlinkability is a key goal for data protection by design, to effect data minimisation and selective disclosure. This has been confirmed by the analysis of Article 25. From the threshold analysis performed, and confirmed through the expert interviews, it was shown that pseudonymisation can accomplish unlinkability when coupled with full selective disclosure. The state of the art in the field of eID has revealed that modern national eID schemes rely on pseudonymous identifiers for unlinkability, whereas more and more national eID schemes recognising the importance of selective disclosure as confirmed by the experts.

However, the current implementation of the Interoperability Framework has not implemented selective disclosure. This omission renders pseudonymisation ineffective in practice. For those eID schemes that rely on these measures, participation in eIDAS will force them to compromise on a high level of unlinkability.

Lowering the level of unlinkability guaranteed by national eID schemes should be considered as opposing the tenet of eIDAS Article 12(3)(c). In addition, lowering the level of data protection by design for cross-border transactions cannot be justified against GDPR Article 25. The current implementation of the Interoperability Framework should be extended to offer a greater level of unlinkability.

A cost-effective and easy to implement solution can be offered through the extension of the SAML protocol used by the eIDAS nodes. This would allow those national schemes that rely on pseudonymisation and selective disclosure to continue to use them even in cross-border transactions. Such a solution is supported by the conducted desk research and has been recognised by the experts as an improvement over the current implementation.

Most importantly, it will increase the level of unlinkability, and therefore the level of data protection by design, supported by the Interoperability Framework, demonstrating meaningful compliance with the GDPR.

[822] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability* (WP 173, 2010) 13: *"A one-size-fits-all approach would only force data controllers into structures that are unfitting and ultimately fail."*

Chapter 11

Conclusion

This thesis explored the impact of the GDPR upon the provision of cross-border eID under eIDAS. Since both legal instruments are of the same legal value, it was determined that both shall apply in cross-border eIDs. The parallel application, however, creates questions of potential tensions between the two instruments. To precisely delineate areas of potential conflict, a systematic interpretation of eIDAS and the GDPR was performed, using a classification framework based on the *ratio legis*. The analysis identified that in the area of data protection by design eIDAS and the GDPR contain potentially conflicting provisions. It deduced, therefore, that the question of impact of the GDPR on the eIDAS framework, as the latter is shaped by the Implementing Acts, becomes a question of determining whether the level of data protection by design afforded by eIDAS' Interoperability Framework meets the standard of Article 25 GDPR. The research question of this thesis, then, is:

Is the level of data protection by design that can be achieved by eIDAS' Interoperability Framework enough to satisfy the requirements of GDPR Article 25?

This question is significant because of eIDAS Article 12(3)(c), which expressly provides that the Interoperability Framework shall facilitate privacy by design. The three LoAs defined under eIDAS Article 8 only partially address data protection by design, i.e. essentially the integrity of the data. In any case national data controllers operating eID schemes are now bound by GDPR Article 25, which also means that their liability obligations under eIDAS Article 11 shall now be combined with GDPR Article 82 (as well as GDPR Article 83). A breach of Article 25 would incur compound liability (and fines) under the combination of eIDAS Article 11 and GDPR Article 83(4)(a).

Having established that the GDPR shall apply in parallel to eIDAS, as indicated by eIDAS Article 5(1), the Interoperability Framework should go one step further than *"facilitat[ing] privacy by design"*.[823] In fact, because the GDPR and eIDAS are two

[823] eIDAS (n 782) art 12(3)(c).

parallel layers of requirements, the Interoperability Framework must satisfy the GDPR's stringent requirements on data protection by design.

Data protection by design under GDPR Article 25 requires data controllers to set up technical and organisational measures to meet their obligations. Data protection by design obligations extend beyond the mere satisfaction of the data protection principles of GDPR Article 5. Instead, they expect a holistic view, one that considers all obligations set forth by the GDPR. When these obligations were organised into groups of data protection goals, unlinkability – the ability to control and mitigate the aggregation of data that can enable the identification and profiling of individuals – was flagged up as potentially problematic.

An acceptable level of data protection by design must implement adequate technical and organisational measures according to the state of the art, the cost of implementation, the data processing and the risks to the rights and freedoms of natural persons posed by the processing. In order to provide a comprehensive answer to the research question a thorough investigation of all these contextual criteria is required.

Having briefly described what the Interoperability Framework is, the thesis highlighted the importance of a data protection by design methodology that can be tailored for the needs of interoperating eID schemes. A first step towards a data protection by design methodology shall be sought within the context of GDPR Article 35, which provides for a process of assessing the risks of processing for the rights and freedoms of data subjects and their mitigation. However, having reviewed the proposed DPIA methodologies from national DPAs, the thesis identified a gap in relation to data protection by design: Since the meaning of GDPR Article 35 is the formation of a risk assessment that can be applied from the design of the processing, i.e. before the processing starts, and in parallel with it, following a DPIA methodology becomes problematic as certain necessary aspects of the processing are only known at a later point in the operation of the scheme (e.g. integration decisions of the receiving Member State; number and identity of actors involved in authentication scenarios and their contractual relationships, as for example in the case of the private-sector Identity Providers of Gov.UK Verify). Therefore, this thesis proposed that a methodology for data protection by design should be informed by DPIA methodologies but should be tailored to identify and assess risk areas in the form of wider data protection goals.

Accordingly, the thesis analysed the requirements, i.e. the data protection goals as per the German SDM model, underlying the principles of data protection by design, in conjunction with conformity to the data protection principles as established by CNIL. To do so both Article 25 as such and Article 35 were covered. Article 35 offers a process to engineer the data protection goals embedded within the GDPR at the time of the selection of the means for processing and thereby a process to identify the control measures necessary to meet data protection goals, in particular in the context of the functioning of an eID scheme. Examining the data protection goals in conjunction with eIDAS, the analysis highlighted that unlinkability is a key data protection goal that serves both data minimisation and purpose limitation. As confirmed by the literature on eID, unlinkability can be achieved by methods such as selective disclosure and pseudonymisation. In fact, this thesis explained that for the purposes of eID effective pseudonymisation can only be achieved if coupled with selective disclosure.

This claim was then tested with an analysis of the state of the art, conducted through desk research targeting 3 national eID schemes. Based on the analysis of the state of the art in the field of eID conducted in chapter 8 and validated in chapter 9 through interviews with experts, it can be argued that the level of data protection by design that can currently be facilitated by the eIDAS Interoperability Framework is not sufficient to meet the data protection goals as embedded within the GDPR. It is true that not all national schemes support selective disclosure and pseudonymisation. However, some do support these safeguards and reducing their applicability to purely domestic transactions seems problematic. In addition, even though eIDAS is first and foremost targeting public sector services, as it was highlighted in the expert interviews, the possibility of involving private sector services[824] is not moot and this prospect should require robust data protection safeguards.

As it follows from the analysis, a way to ensure a higher degree of data protection by design for cross-border eID and authentication would require increasing the degree of unlinkability. The Interoperability Framework is currently hindering what is possible by the state of the art in the context eID schemes in at least two ways:

- First, by making eID a condition of authentication, and therefore requiring the unique identification of individuals. Uniquely identifying an individual should only be required in a limited number of use cases, in the initial operation of cross-border transactions and mostly for public services.
- Second, by specifying a Minimum Dataset of identifiers and a unique identifier *"as persistent as possible in time"*.[825] The Interoperability Framework lacks flexibility. The presence of a defined set of identifiers precludes any ability to select which data to transmit according to the needs of the Service Provider. Besides the use

[824] As indicated in eIDAS (n 782) rec 17 *"Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions."* See also eIDAS Observatory, *Principles and guidance on eID interoperability for online platforms* (final draft, 2018) ⟨https://ec.europa.eu/futurium/en/system/files/ged/draft_principles_eid_interoperability_and_guidance_for_online_platforms_final_draft_june_2018.pdf⟩ accessed 3 September 2019 (archived at ⟨http://archive.fo/Nx1Ua⟩) 2: *"The aim will be to encourage online platforms to recognise other eID means – in particular those notified under the eIDAS Regulation (EC) 910/2014 – that offer the same reassurance as their own"*.

[825] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions on the internal market [2015] OJ L235/1, ANNEX 1(d).

of pseudonyms in the current implementation, absent the ability to selectively disclose attributes, is limited to serving as mere replacements of persistent unique identifiers.

The above limitations, although in contrast to the state of the art, could potentially be justified against the nature, scope, context and purposes of processing. In other words, if eIDAS were to be limited to public administrations one could argue that all public services would in practice require the attributes of the Minimum Dataset to successfully distinguish between individuals. Such a claim has been contested by some of the experts during the interviews. Nevertheless, eIDAS has shown a clear aspiration to extend its eID services to the private sector. In private sector services, e.g. in online social platforms, unique identification is not a precondition for effective delivery of the service. Consequently, unique identification in these services would unnecessarily increase the risks to the rights and freedoms of the users. If eIDAS were to be extended to private sector services, the omission of a high level of unlinkability would be difficult to justify.

In addition, the omission of support for a high level of unlinkability is troublesome when considering the participating national eID schemes. For eID schemes that rely on a high level of unlinkability, participation in the Interoperability Framework would effectively mean that these eID schemes would not be able to guarantee the same level of data protection to their users. Actively forcing participating national schemes to lower the level of data protection supported goes directly against the substance of eIDAS Article 12(3)(c) and, as has been established, cannot be justified neither against the state of the art, not against the nature of the processing.

GDPR Article 25 allows for consideration of measures also against the cost of implementation. It is arguable whether economic considerations can be the sole reason justifying a lower level of unlinkability.[826] In any case, this thesis considers the point moot by demonstrating that implementation of a higher level of unlinkability does not come at a higher cost.

The thesis proposes a practical solution that would allow the eIDAS-nodes, i.e. the translating layers between a national eID scheme and the Interoperability Framework, to implement functionality for selective disclosure and pseudonymisation. National eID schemes and services providers communicate through intermediary eIDAS-nodes. The

[826] The EU Parliament has already opined that the implementation cost should not be the only consideration: EU Parliament: Committee on Employment and Social Affairs, *"Draft Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* (C7-0025/2012 – 2012/0011(COD), 8 November) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); see also Article 20 of Dir 2016/680 which replicates Article 25 of the GDPR albeit it its elaboration in recital 53 of the preamble to the Directive where it is stated that the implementation of the measures referred to in Article 20 *"should not depend solely on economic considerations"*: ibid rec 53.

eIDAS-nodes use the SAML protocol to exchange authentication data between them (as well as between the node and the national scheme or service provider). An extension of the SAML protocol used for the communication of the eIDAS-nodes could allow them to support such functionality for those participating national schemes that rely on them. The extension can be implemented via a Technical Standard, so that no further legislation or policy change is necessary. Importantly this would keep cost to a minimum, provide better unlinkability within the Interoperability Framework and ensure the compliance with GDPR Article 25. The result would be true *"facilitat[ion] of privacy by design"* as per eIDAS Article 12(3)(c).

Summarising the contribution of this thesis, it demonstrated that data protection by design should be thought as a continuum, whereby the level of protection that eIDAS must achieve will be equivalent to the benefits and risks of processing, the cost of implementation and the state of the art. However it discovered that a suitable methodology to assess the level of data protection by design is absent. To address this absence, the thesis formulated a tailored threshold analysis specifically for data protection by design. The threshold analysis was inspired by the developments in data protection impact assessments. The adapted threshold analysis was tested against eIDAS' Interoperability Framework. Based on the results, the thesis argued that the level of data protection by design that can be achieved by eIDAS' Interoperability Framework is not enough to satisfy compliance with GDPR Article 25, especially in regards to unlinkability. National implementations of eID have already began moving towards a high level of unlinkability, to ensure adequate separation of datasets between sectors and protect against profiling. Participation of such schemes in the Interoperability Framework will result in the lowering of the level of data protection by design that they have guaranteed to their citizens. It was stressed in this study that lowering the level of data protection by design should not only be seen as a violation of GDPR Article 25, but also as going directly against the instruction of eIDAS that the Interoperability Framework shall facilitate data protection by design. To mitigate the Interoperability Framework's failure to meet the standard of the data protection by design, the thesis proposed a practical solution to enable participating schemes to achieve a high level of unlinkability.

Appendices

Appendix A

Notification status of national eID schemes

Country	Name of the scheme	Name of the eID means	Level of assurance	Notification status	eIDAS MDS (mandatory)				eIDAS MDS (optional)					Additional attributes (non eIDAS MDS)				
					Current family name(s)	Current first name(s)	Date of birth	Uniqueness identifier	First name(s) at birth	Family name(s) at birth	Place of birth	Current address	Gender	Nationality	Passport number	Email address	Mobile phone number	Other
Belgium	Belgian eID Scheme FAS / eCards	Belgian Citizen eCard Foreigner eCard	High	Notified	X	X	X	Derived from the National Register Number			X		X					
	Belgian eID Scheme FAS / Itsme®	itsme® mobile App	High	Notified	X	X	X	Derived from the National Register Number			X		X					
Croatia	National Identification and Authentication System (NIAS)	Personal Identity Card (eOI)	High	Notified	X	X	X	Derived from Personal Identification Number		X	X	X	X					
Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	Notified	X	X	X	Derived from Person Identifier Number			X	X				X	X	Country Code of Birth Age ID Type ID Number
Denmark	NemID	Key card (OTP); Mobile app; Key token (OTP); NemID hardware; Interactive Voice/Response (OTP); Magna key card (OTP)	Substantial	Notified	X	X	X	Derived from Denmark's unique 10-digit PID number			X	X (for people residing in Denmark)	X					
Estonia	Estonian eID scheme: ID card Estonian eID scheme: RP card Estonian eID scheme: Digi-ID Estonian eID scheme: e-Residency Digi-ID Estonian eID scheme: Mobiil-ID Estonian eID scheme: diplomatic identity card	ID card RP card Digi-ID e-Residency Digi-ID Mobiil-ID Diplomatic identity card	High	Notified	X	X	X	Estonian personal identification code			Found only on ID card and RP card		Found only on ID card and RP card	Found only on ID card and RP card				
Germany	German eID based on Extended Access Control	National Identity Card Electronic Residence Permit	High	Notified	X	X	X	Pseudonym	Joint attribute		X	X						
Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	Notified	X	X	X	Derived from Tax Code										
	SPID - Public System of Digital Identity	SPID eID means provided by: Aruba PEC SpA Namirial SpA InfoCert SpA In.Te.S.A. SpA Poste Italiane SpA Register.it SpA Sielte SpA Telecom Italia Trust Technologies S.r.l.	Low Substantial High	Notified	X	X	X	Derived from SPID Code		X	X	X	X		X	X		Tax identifier for the Italian citizens
Latvia	Latvian eID scheme (eID)	eID karte eParaksts karte eParaksts karte+ eParaksts	Substantial High	Notified	X	X	X	Derived from personal identification code										
Lithuania	Lithuanian National Identity card (eID / ATK)	Lithuanian National Identity card (eID / ATK)		Pre-notified														
Luxembourg	Luxembourg national identity card (eID card)	Luxembourg eID card	High	Notified	X	X	X	Derived from Luxembourg's national identifier number			X	X (Only for citizens residing in Luxembourg)	X					
Netherlands	Trust Framework for Electronic Identification (Afsprakenstelsel Elektronische Toegangsdienstent)	eHerkenning (for business) Idensys (for citizens)	Substantial High	Notified	X	X	X	Derived from Burgerservicenummer (BSN) (Citizen Service Number)			X	X						If requested by a relying party: VAT number; tax reference number; Legal Entity Identifier; Economic Operator Registration and Identification Number; excise duty number
	DigiD	DigiD Substantieel DigiD Hoog		Pre-notified	X	X	X	*Unknown**	X	X	X	X	X	X				
Portugal	Cartão de Cidadão	Portuguese national identity card (eID card)	High	Notified	X	X	X	Derived from Civil Identification Number				X	X	X (if authorised by citizen)				
	Chave Móvel Digital	Digital Mobile Key	High	Notified	X	X	X	Derived from Civil Identification Number				X	X	X (if authorised by citizen)				
	Sistema de Certificação de Atributos Profissionais	Professional Attributes Certification System	High	Pre-notified	X	X	X	Derived from Civil Identification Number				X	X	X (if authorised by citizen)				
Slovakia	National identity scheme of the Slovak Republic	Slovak Citizen eCard Foreigner eCard	High	Notified	X	X	X	*Unknown**		X	X	X	X	X (scheduled for future)				
Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	Notified	X	X	X	Derived from National Identity Document Number										
United Kingdom	GOV.UK Verify	Gov.UK Verify eID means provided by: Barclays Experian Post Office SecureIdentity Digidentity	Low Substantial	Notified	X	X	X	Derived from an Identity Provider					X (if disclosed)					

TABLE A.1: Overview of pre-notified and notified eID schemes under eIDAS on 24 September 2019[a]

[a] Correct as on 28 May 2020. Compiled from the sources at: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS. Archived version at: https://bit.ly/2B0UIWA.

Appendix B

Interview transcripts

Transcript Keys

Interviewer:	INT.
Interviewee:	RESP.
Timestamp:	🕐
Redacted personal data:	[name]

B.1 Austria

INT. Let's try and record this. I'm going to be recording the sound, by the way, if that's alright? 🕐00:00:00

RESP. Yes, that's fine. That's fine.

INT. Brilliant. Thanks for taking the time. Right, I've gone through your answers. Really helpful. So I think it'd be best if we just focus on selected issues, rather than go all through the questions again.

RESP. Fair enough. It's your show, so, [overtalking].

INT. You are talking about eID replacing the citizen cards. Could you tell me what the difference between the two is going to be?

RESP. Okay. The replacement… This replacement basically is that the term citizen card was not too useful. We refer to a citizen card as a technology neutral concept. Both smart cards, or mobile ID, or whatever fulfils the requirements. But with the term citizen card, anyone always thought of an ID card, a physical token like credit card size, or a smart card, and so forth, even though it wasn't meant that way. So, the first change was no longer talk about citizen cards, because… 🕐00:01:23 Not sure whether I mentioned that in my responses, but smart card type citizen cards quote unquote are rarely used by the citizen. We currently have close to 900 000 mobile eIDs. And the health insurance card, which is issued to nine millions, but the eID function has just been activated by now went down to 26K. So the citizen mainly uses the mobile eID. But that mobile eID is also called citizen card, so the term card doesn't fit. That is the change in terms of terms, terminology. And with eIDAS, and also with the experience we had with the previous system, we did some architecture change. Like Austria was a decentralised system called middleware out of STORK. The… Which was fine with larger data centres because they could easily install and maintain the middleware. And also when we started the project, there was little integration in of the [unclear] product, of the shelf products like into an IBM [unclear] server, or whatever you use as… Or into WebSphere or whatsoever. Meanwhile summary based integration is a standard, so the integration, in particular for small units, for [unclear] it's easier when we provide a central authentication gateway, like an Identity Provider. And that is the major architectural change. Also for the cross-border handling, it is easier to have the centralised system, rather than the decentralised. Even though one of the reasons for going for the middleware model for the decentralised system was data protection.

⏱00:03:51 INT. Yes.

RESP. Because the data controller deploys the software getting hold of the personal data, and there is no search party in between. So in the new architecture, for instance, attribute provisioning gets more complex technically, as to maintain the same level of data protection. We need assertion encryption , and end to end encryption of attributes if we query an attribute from another register, the central system shouldn't get aware of that. So that makes it more complex technically. But we didn't want to do that change with refuse [unclear] data protection measures.

INT. Yes.

RESP. Because the original system was… Also the law was develop [unclear] corporation with the data protection authority. So those are the main changes making a key… A more abstract term, eID, so that no one thinks of a card, when you talk about citizen cards and cards aren't used any longer, and the architectural change.

INT. Does that mean that every municipality is going to be an Identity Provider, or it's going to be just one server, one portal?

RESP. No. That will be one portal. Basically the Identity Provider is the… Or identity
⏱00:05:11 provision is based on the… Central… Central population register.

INT. So it's going to be the S PIN authority then?

RESP. Well, it's a bit more complex because the population register is the minister of interior, and the actual Identity Provider is then, what is called the Source PIN authority, which is the data protection authority. The data protection authority queries the population register, the population register has a unique identifier in there. But the data protection authority encrypts that identifier to what we call a

Source PIN. The reason is if there is, as we explained, or as I explained later, we have a sector specific system, and which doesn't mean that we wanted to create silos, like social security tags entails. But to facilitate an E-Government where there is a legal basis for data sharing, the data protection authority can create the links between the identifiers. But the ministry of interior probably isn't the most trusted on that in the perception of the citizens.

INT. Yes. 00:06:46

RESP. The highest authority quote unquote, we have in terms of maintaining privacy is the data protection authority. So even though technically this was operated by the ministry of interior, it is… The controller there is the data protection authority. And in terms of the data protection directive, the ministry of interior would be the processor, but under supervision, and control of the data protection authority.

INT. So, just to fully understand it. Under the previous system we had two actors. We had the user, and we had the Service Provider. And the user…

RESP. Yes.

INT. Would authenticate against the Service Provider directly.

RESP. Yes, exactly.

INT. Whereas under the new system, is the user, the Service Provider, and added the S PIN authority?

RESP. Exactly . And under the old system, data was stored on the credential, like
that Source PIN, that encrypted identifier was stored on the card for instance.
Or if it was the mobile eID, which is also a sort of a central system, operated
by a qualified trust Service Provider, the card quote unquote, was held by a
Service Provider on behalf of the citizen. But the data was stored there. And
the sector specific identifiers was… Were calculated with every authentication in
the requirement of the citizen, like software the citizen runs, or at the mobile eID.
And that however requires, unless you define or create specific requirements, like 00:08:38
for the smart card, like Germany people, with the NBA creating such application
specific identifiers, in the case of Germany, on the card. That requires specific
cards, which is costly. Which probably is more efficient in a country like Germany
with 80 million population. A smaller country, like Austria, we rather went for
standard cheap operating systems. And also high level requirements, which then
however requires that the software running on the PC reads the Source PIN,
does the calculation, and forwards it. And now we create that identifier. Or the
data protection authority now creates those sector specific identifiers with every
authentication in the computing centre. Which then also means that the most
critical part, that Source PIN, actually never leaves the data protection authority
as a controller, just the sector specific ones. So…

INT. And so the S PINS are communicated. The S PIN stays in the data…

RESP. Use a central system, yes.

⏱00:10:22 INT. Sorry.

RESP. The outcome of course is in theory there is a tracking possibility by that central component.

INT. Sorry, your image has frozen for a bit. I only got the tracking possibility. But which component is trackable? Are we... Have I lost you? Why? Why? Sorry, of course...

RESP. Hi, did you...

INT. Of course there would be network problems. Of course. I lost you when you were saying about a tracking possibility of the central component.

RESP. Yes. Well, in fact with the central component , in theory you always have the tracking possibility. There are security measures like excursion [unclear] encryption, so that the central component doesn't learn which attributes are requested, and so forth. But still there's a central component. On the other hand, what we introduced, or what we could introduce with the new architecture, or will introduce, it's not in place yet, it's currently being implemented. What we could introduce is that the citizen herself can see the locks so that she can access all her eID activities, and... To see whether there was any compromise, or the card she lost, together with her pin probably, was used in a service. So there were pros and cons, and the original idea of a decentralised system was due to data protection, and also due to liability reasons. With no third party involved, there is no liability issues. It's always the user acting with the Service Provider. On the other hand, we could gain some security measures, and additional security features, or privacy features
⏱00:13:42 like the locking possibility and so forth.

INT. Yes. In your answers you referred to qualified trust Service Providers. In the Austrian system, is that for the combination of a card and a card reader, for example? Does that count as a qualified trust Service Provider, or are we talking about a third party service?

RESP. Okay, that... It's always a third party service, and it's a qualified trust Service Provider issuing qualified certificates. As in the Austrian system, the eID is closely linked to qualified electronic signatures. Whenever I authenticate the service, I give with the qualified electronic signature, and be full act up front, and in the response there's even a screen shot which says what I'm signing, really signing, is a qualified electronic signature. Basically saying I want to do business with the
⏱00:14:57 tax authorities. And with that qualified electronic signature up front, we even could reduce the number of [unclear] that we used to sign on paper. Where the signature of... Just was the wilful act to submit a tax declaration for instance, just as an example. And with that wilful act upfront, many services no longer needed a signature on the transaction itself. Other services still need it. Like when you apply for retirement or a banking service where the transaction is signed. That

uses the authentication function, including a qualified signature upfront, and finally signs the transaction. But as we often have the case where I need authentication or eID to enter a service, and an electronic signature to compute it, we closely linked those two functions already in the architecture, and in the design. And so whatever the token [unclear] is, it requires a qualified electronic signature, which requires a qualified trust Service Provider. And with the mobile eID that uses the remote signing functions that were clarified under eIDAS, there Annex three anyhow says that if such a remote qualified signature creation device is used, it must be operated by a qualified trust Service Provider. That's one of the requirements in Annex three of eIDAS. And therefore the mobile eID, which is mainly used aside some profession cards, like lawyer cards, or lottery cards, the mobile eID anyhow needs to be operated by a qualified trust Service Provider. And with that success, then uses them, also strong relies the new eID system for the authentication function in online services. Still strongly relies on a qualified trust Service Provider.

INT. Right. ⏲00:17:31

RESP. But also it's new in the system, I'm not sure whether I responded that. We also introduce offline authentication, or identification functions, like a smartphone app where you can show your driving licence, or an ID card on a smartphone app. But we… Both is called eID, because for the citizen, it's the same function, the same tool whether I have the driving licence on the phone, or whether I authenticate online, the… Still the phone is used. But the conceptual function is different, whether to enter an online service. Or whether you use it, for instance when buying cigarettes to ensure identification [unclear], because that will be the first pilot likely launched still this year of that new function under the new law.

INT. But in that case, in the case of offline authentication, then that means that no SS PIN is transmitted. Or is the SS PIN already stored on that device?

RESP. Okay, I now have an acoustic problem. You would need to repeat that one.

INT. Yes. In the case of offline authentication, how is the SS PIN calculated, because obviously you don't have an online link to the S PIN authority?

RESP. Okay. There offline probably was the wrong word. It rather is [unclear] presence, ⏲00:19:16 because nowadays with the smartphone, we assume an always online function. So there is an app, the app is paired with functions of the register. Like identity document register, and there also, the online function is legally, it's just a service, like the secret booth is offline. You show your mobile phone to do the age verification.

INT. Okay, got it. Can we talk a bit about eIDAS interpretation? If I understand your answers correctly, every member state is going to receive one sector authenticator.

RESP. Exactly, yes. So, within Austria the identifiers per sector are different. Under the territorial principle already under the data protection directive, we however cannot impose that identifier, for instance in UK, also is derived sector specific.

Or in Sweden, Sweden uses unique identifier flat across systems. As soon as the identifier passes the border, Sweden is the controller. And we just say each member state, or international organisation, like with the [unclear], the European Union for us, authority commission is one international organisation, gets a sector ⏱00:21:24 specific identifier. Whether that identifier is used by the commission flat across all services, or in UK flat across services, or whether there are national measures to also have additional data protection technologies introduced, that's up to the receiving member state.

INT. Right.

RESP. What we just do not want is that we create the one identifier for Sweden, and at the very moment of authenticating the purpose of data processing is an Austrian accessing a Swedish service. And that later on, the identifier gets shared without knowledge of the service.

INT. But doesn't that mean if Sweden gets only one identifier for every public service they have, doesn't that mean that basically all public services in Sweden can share that identifier amongst each other? So doesn't that in a way…

RESP. Exactly.

INT. Lessen the security of the Austrian system?

RESP. No, not the Austrian system. That's not our business, not our responsibility, because Sweden already shares their identifier for a Swedish citizen when doing services in Sweden. Or if I migrate to Sweden as an Austrian, I receive a permanent identifier in Sweden. That's up to the… That's the Swedish authority's business, and the Swedish data protection authority's business to assess whether such… Such ⏱00:23:16 sharing is compliant with the Swedish law. On the other hand, if we receive an identifier, it's our sovereign decision that the Swedish citizen receives the beauty of sector specific identifiers within Austria. And it's not up to Sweden explaining us that we should share identifiers of Swedish citizens between Austrian services. That's [unclear] Austrian data protection authority in charge of that.

INT. Yes, I understand that these are matters of sovereignty. But speaking from a data protection point of view, from a security point of view, regardless of what state you're from, or what state you're going. Having only one sector identifier is more prone to linkability than having multiple sectors, right?

RESP. Yes. Yes. It is. That's why we in Austria decided to go for sector specific identifiers. We would have loved… Or for instance, in Austria we do not include the identifier. This identifier in qualified certificates for signing as we argue that also is a scope creep of the signature function, because signing a document is just authentication, and no unique identification. So we would love other member states to do that similarly. But Estonia, Spain, and so forth, decided differently. And even though we think that our system is the greatest in the world, the same goes for Sweden or Estonia.

INT. You are saying in your answers that the minimum data set is always transmitted. There could be scenarios where that is not needed, right? So, right now you talked about re-authenticating or signing a document which doesn't necessarily need your [unclear] data set.

RESP. Yes. 🕐00:25:38

INT. Is there a… Also you're saying that in future, in the eID scheme that is coming in Austria, maybe that kind of selective disclosure is going to be possible.

RESP. Yes.

INT. This is not possible right now the way eIDAS operates, correct?

RESP. Exactly. I mean that was discussed in, that was discussed in the council and also in the expert [unclear] technical subgroup. And the compromise given that, for instance, some member states do not have the system identifiers, or have several identifiers. The compromise basically is, and Austria was fine with that, because that was also the computation [unclear] with the data protection authority we had when drafting our law, is… Well the name and date of birth is data that is needed in most services. There are cases like age verification, or… Well, adult services, or whatsoever where pseudonym was or [unclear] services… Are you still there, because…

INT. Yes.

RESP. The… Okay, good. Just the video. 🕐00:27:08

INT. Yes.

RESP. I suppose. Okay. And aware that there are services that… Where it wouldn't be needed, but the compromise basically was to have the minimum data set. In the technical subgroup, we are discussing the possibility that to amend the specification in a way that if a service doesn't request the minimum data set, that you just can deliver the first name, for instance, and things like that. But the current specification refrained from that, and I strongly supported that. In particular to make sure that the initial deployment was, yes, this works. For instance that the citizen cannot opt out to… Of delivering the minimum data set. Like many member states, like Austria, for inbound services enrol the citizen, or assign a national identifier, also in the eIDAS case, so that the semantics for instance is the same. And to decide whether a citizen has been enrolled already, in particular for those member states that do not have persistent identifiers, like Germany, and I need a set of attributes where I have sufficient probability to know whether the citizen was enrolled or not. Assuming that in five years eIDAS is a success, that services are enrolled, of course, from a data protection perspective, it would be great if the Service Provider just requests the date of birth, or the year of birth to just deliver that. But for those countries that use the eIDAS minimum data set to…

Also to check whether a citizen's already enrolled, we somehow need that data to get eIDAS flying. So the current approach of eIDAS is minimum data set this, minimum data set, it needs to be delivered. And that, that's the compromise we ended up with.

00:29:52 INT. Yes, understood. Well from what I understand, and I'll have to verify that with Detlef [unclear] probably. But the way Germany has pre-notified the system, they're going to be assigning a persistent identifier to…

RESP. No.

INT. Is it going to change…

RESP. No.

INT. In every authentication?

RESP. Not yet. Not in any authentication, but the issue quote unquote with Germany… I have been in [unclear] your theme of the German system, so I'm pretty aware what the system is about. The identifier for public services, because Germany distinguishes between the public and the private services, for public services, the
00:30:46 identifier remains the same. For a receiving member state, like with Austria, for the validity period for the duration of a card, if a card gets replaced, the citizen gets a new identifier. And that is one of the cases where we need the minimum data set, and also the optional data, which… Because Germany will not only deliver the minimum data set, in addition to the name, also the name at birth is communicated, and name at birth is persistent, and the place of birth. And with the place of birth, you have a very high probability that based on the minimum data set, and the optional data, that you just have a unique match. Like in Austria, we are nine million in Austria, amongst the nine million, we have just 600 digital twins based on name and date of birth. And if you add the place of birth, in Germany, Berlin is the biggest city, so given… Doing the math, it's not just a third, but the probability is much less than having a few hundred, there may be a few. But such cases can exist.

INT. Yes.

RESP. And in those countries that rely on [unclear], if I ask if all their processes aligned with that, so that they need somehow to do the fade over from the old card to the new card, and therefore the optional data is used per journey.

INT. Yes. But even in that case, that means that the minimum data set is needed only when replacing the card. So, let's say every four years, or in case you lose it. But in the meantime…

00:32:56 RESP. Yes.

INT. You could have transmitting only the unique identifier, right, after the first initial identification?

RESP. Exactly. Yes, exactly.

INT. Can I ask you something about multiple eIDs? You said that it's possible in Austria to have multiple eIDs. So in the form you can have a card, and you can have a mobile eID. Do these have different S PINS, or do they all share the same S PIN?

RESP. The identifier is the same. The sector specific identifiers are the same, because the calculation of the source PIN is done the same, and is stored on the same card. The only thing what we need to do is the multiple identifiers, because the qualified certificate is different. That even could be by a different...

INT. Provider.

RESP. Certification Service Provider, for instance. We need to link the identifier with the certificate. And as I said, we do not include the identifier in the certificate, because for us that would be a privacy nightmare, more or less. In the issuance process, what is done is that the data protection authority signs the assertion that this identifier is linked to that certificate. And the validation process, that includes the verification of that assertion to make sure that you do not enter your card to deliver the identifier. And then use a different card of someone probably called Nico, to sign. Because the name still is in the certificate, but that link is a bit weak.

INT. Yes. 🕐00:34:59

RESP. You can't find two Nicos that share the certificate. And so that is one of the measures in the issuance process that a certain certificate is linked to one identifier. And if I have multiple eIDs, like I have, I think I have four, three smart cards, three active smart cards and the mobile eID. All those eIDs have the same identifier, but different qualified certificates.

INT. But... So, does that mean that the Service Provider that you're authenticating against, can they differentiate between which ID you use to authenticate, or does it appear as one thing?

RESP. Yes. Okay, in theory the Service Provider can, or in practice he can also. Like the mobile eID is A, under a different route of the PKI [unclear] the smart card eID. All smart cards share the same route. So the Service Provider cannot distinguish whether I use the health insurance card or a bank card. But the distinction whether I use a smart card, or a mobile eID currently anyhow can be made by the Service Provider, as when I authenticate, I need to select what type of eID I'm using as a citizen, because the Service Provider doesn't know. In the new service, with a central system, it... The Service Provider might not learn that, but at least the 🕐00:36:46 central system needs to know which... What to use. In particular as the system remains open for several tokens, which is pretty common. Like a public servant or a lawyer has to have an eID, because all filings to courts in Austria are done electronically. However, that is a very specific certificate also saying I'm a lawyer, and the same lawyer wants… Doesn't want to use that certificate in his private life, so for such cases, you may have several eIDs.

INT. So in the new system, does it mean that the central component, I'm understanding it will function a bit like a hub, like a middleware between the user and the… So…

RESP. Yes.

INT. Does it mean that that central component is going to know where a user is deploying their eID? So it's going to be able to link between users.

00:37:59 RESP. Well, in the… In… Basically, yes, it can. Again there are legal measures that that those data may only be stored for displaying that to the user, to see the history. But basically as in any identity system that uses the Triangle IDB [unclear] Service Provider and user, unless you have processing at the user device, somehow learns who is the Service Provider.

INT. Yes. So, in an eIDAS environment, you said probably the proxy configuration is going to be used. Does that mean the same central component that is used domestically, or they're going to deploy a proxy in every member state?

RESP. Yes. Well, we… There will be the central component domestically. However, given that we have some 300 services that currently use the middleware model, there needs to be a seamless migration. So, those Service Providers that currently run middleware, and have integrated that, simply instead of accessing the citizen card environment, as we call it, will with the next version of the middleware send an authentication request to the central component. For those services that migrate fully to the new system, as it is a pretty general sample profile we are using. They might use the integration they already have in their system, their WebSphere server, their [unclear] server, whatever they use as it is a standard sample protocol we are using. Like eIDAS is using a standard sample protocol .

00:40:28 INT. Yes. So in a scenario where I am in the UK, I'm an Austrian citizen, I want to identify using my Austrian eID. Will that identification go all the way back to Austria, or there's going to be a proxy in the UK?

RESP. In… As UK and Austria, will use… We'll both use the proxy model, it's the latter. There are two proxies. The… And segmented trust relationships, the UK Service Providers just trust, or need to trust the UK proxy. So the UK service, let's say… Well, department of work and pensions, or whatever it is. I as the… What was your case? Austrian citizen, UK service? Okay.

INT. Yes.

RESP. I access the UK Service Provider, and they'll click authentication, and probably even click as it's… Well, let's assume that eIDAS is not fully integrated with [unclear] dot gov for instance, then I would imagine that the UK service has two partners [unclear] dot gov, or I'm a European citizen. When I click [unclear] dot gov, that's the standard process. When I click I'm a European citizen, the service will redirect using an… A standard authentication request to the UK gateway, or the UK proxy. And let's assume UK deploys it that way, that the country selection is done at the proxy, because both ways are possible. Or I can select I'm Austrian at the Service Provider, but the redirection to the UK proxy stays. So, at the UK proxy, I select I'm an Austrian, so the UK proxy redirects to the Austrian proxy, which then in our case is already the central service. And that central service then redirects the authentication to the qualified trust Service Provider. Because it can be several.

INT. Yes. ⏱00:43:13

RESP. So you have two trust, three trust relationships. The trust relationship is between the Service Provider and the connector. Then the proxy, that proxy is called eIDAS connector. So connector is always the system talking to the Service Providers. Then you have the trust relationship between the… Between all the proxies, and the national trust relationship between the Austrian proxy and the service. So that is the segmented trust relationship. Also with, I mean the, the downside of the proxy system is there is no technically enforced end to end security. Because if one proxy is hacked, whether it is the Austrian or the UK proxy, it either can authenticate with UK service. Or if the Austrian proxy is hacked, it can generate [unclear] Austrians, quote unquote. Because the UK proxy just signs an assertion someone has authenticated further.

INT. Yes. Would it be… Would it help in that case, since end to end encryption is not possible, I guess. Would it help if selective disclosure was a thing that could be applied? So would it help if the Austrian central component could only send some attributes instead of all attributes to the UK proxy?

RESP. Well, actually not in the case a system gets hacked, because if the… If either of the proxies gets hacked, I would request… I would overrule the selective disclosure by requesting the minimum data set as through mandatory services. ⏱00:45:04

INT. Well…

RESP. Because selective disclosure also requires that the Service Provider says ID'd.

INT. Yes.

RESP. And, and the identity [unclear] just discloses what is needed.

INT. I guess it depends on the hacking, because it doesn't have to be impersonation, it can be just snooping the traffic, right?

RESP. Okay, on snooping the traffic, the eIDAS protocol, the cross-border protocol does assertion encryption. In particular as we rely on each deposed and redirect findings. Which means all the data passes the browser. So the assertion between the proxies gets interrupted, so snooping on the line, or snooping the browser doesn't help you in the cross-border section. However, eIDAS did not interfere with the deployed systems, it is up to the sending member state, and the receiving member state whether assertion encryption is applied. Austria will do so if UK does the same. There will not be end to end encryption, because with the segmented trust relationship…

⏱00:47:00 INT. Yes.

RESP. You always need to re-sign the assertion. And the key management is a nightmare if you need to do it cross-border, because then you need the trust relationship end to end also. That's why you have that segmented trust relationship. I do not want to get… As Austria, I do not want to know what the key management in UK is, that's your business.

INT. Yes.

RESP. So, assertion encryption is done, but as we cannot interfere with the deployed system just because of eIDAS, because then no member states will have agreed. It is up to the sending and receiving member state what protocols, what security measures are deployed nationally.

INT. Okay. One last one, and then I'm going to leave you to go back to your work. The GDPR says… So this whole interview is happening because we're trying to figure out what the balance is between what controllers have to do, and what they can get away with. So the GDPR says that you need data protection by design, and if we are understanding what they mean by data protection correctly, that means data minimisation, some kind of data minimisation, and technical measures for that data
⏱00:48:34 minimisation. So if that's the case, can selective disclosure, and pseudonymisation be viewed as techniques for that data minimisation? And if they can… Sorry my watch is talking to me. And if they can't be viewed as techniques, then… God, where… Yes. Since at the moment they can't really be applied to eIDAS, the way eIDAS now operates, does it need them? Can it get away without them? Does it make sense, the question?

RESP. Yes, it makes sense. It… I would, however, a bit distinguish here between public services, and private sector services. Knowing that there are public services, like let's say, a drug abuse register that are highly sensitive, and likely won't need the name, and shall not have the name, like to create episodes. Still also in other member states, or I guess in many member states, the name and date of birth is used in most public services.

INT. Yes.

RESP. And their data… Selective disclosure on top of course is helping in terms of data minimisation. I would just argue that in public services, in practice, you have just a limited set of services where… That are relevant. And considering for instance, what are the main cross-border cases you have there. I don't know whether you know that study, there was a study on the main potential, the cross… Of cross-border services. There… It is for instance, student mobility…

⏱00:51:02 INT. Yes.

RESP. Work immigration. Health, eHealth for instance could be something where less data could be useful, but still most hospital information systems ask for the name and also the age and date of birth. But those services that we are mainly looking at as the early adopters, need that minimum data anyhow.

INT. Yes, no...

RESP. As services which are...

INT. Sorry, yes. I understand that, it just at the same time, the commission is issuing reports where they encourage private services, and even worse, online platforms to use eID. So...

RESP. Yes.

INT. A scenario with Facebook is going to get your minimum data set.

RESP. Yes. Yes, exactly. And that is why I did distinguish with private services, because Germany, for instance, already made that decision by asking... By saying our NPA [unclear], the... Our eID can be used by private services, but under the same conditions, like German Service Providers. Meaning that UK private service needs to apply for an access certificate for the German eID, and needs to describe why certain attributes are needed. So with the German eID, Germany already made exactly that decision. For public sector we are fine with the current minimum data 00:52:47
set, as we understand it is needed by most services. But for the private sector, the technical selective disclosure mechanisms that apply to German Service Providers also apply to Service Providers abroad. So, a gaming site in UK may just get an access certificate for age verification, even no identifier.

INT. But how would that work? Would that work over the eIDAS node? So... Or do we need to modify the nodes?

RESP. Technically no problem. It would work. It is just for the initial deployment, and as we do not yet know what other member states make as conditions for private sector use. We have the clause in eIDAS, but just one notification for the moment. We did in the technical specifications not yet tweak based on anticipated conditions. And the... For the moment, it just for the nodes, and for the specification, it just is a practical decision saying for the public services we need it anyhow. But the nodes anyhow get the information whether it is a public Service Provider, or a private Service Provider. And if the issuing member state decides that private 00:54:29
sector providers, for instance, may only get a subset of the minimum data set, then it's... That's a few line of codes saying, if Service Provider is private, make A B C, for instance, optional, and allow the citizen to deselect, or even not to transmit. That's up to each member state, because either says private service... For private Service Providers, as a notifying member state can make conditions, whatever that condition is.

INT. Right. So, the only reason why public services are not asking for separate certificates like private services is because it's up to the foreign member state to decide on that, right? That probably didn't make any sense. I should probably rephrase that.

RESP. Not sure whether it's rephrasing, I again have an acoustic problem. So…

INT. Right. So, we've said at the beginning that the foreign member… it's up to the foreign member states of how they want to organise their public services, which is why most notifying member states choose to deploy one identifier per member state, rather than one identifier per Service Provider. But it will be technically possible to do one identifier per Service Provider, there's no, like, technical overheads that is stopping that, right? It doesn't require excessive computing power, or something like that.

00:56:23 RESP. No. It is technically possible, but eIDAS to some extent is hindering it through the as persistent as possible clause, because if I then derive per Service Provider, it… I wouldn't do my best the possible in terms of persistence. And many member states would have major issues as their way of service provisioning, like on a tax portal, on data sharing with a legal basis, would not work. So they couldn't provide the same service as they do for citizens. And what it also would require, to have a unique identifier per Service Provider is that you have unique identification of the Service Provider itself. Currently we just give a Service Provider name, mainly for the user interface, for displaying it at the user interface. So that at the eIDAS node, you can in the authentication process display a line along UK tax authorities…

INT. Yes.

RESP. Want all… Amazon UK wants to authenticate you.

INT. So the identification doesn't work both ways, that's what you're saying.

RESP. Yes, and to derive a unique identifier for Amazon UK, I would need to know whether there is Amazon UK in terms of the big Amazon, or whether there is a small barber shop in UK called Amazon. And currently we do not require the member states to deliver to the requesting member state [unclear] unique identification
00:58:50 of the Service Provider, because that's a further level of complexity. As if the Service Provider is a ministry, for instance. After each election, the identifiers might change, because we usually change, after elections, responsibilities in terms of who is responsible for social security for instance. But also with private sector Service Providers, what is the quality, for instance, of Service Provider enrolment into the system? Like in UK with [unclear] self-declared commercial registers. So that complexity is currently not in eIDAS. Just if you authenticate as a legal person, there you have the levels of assurance. But not for the Service Provider, that's just whatever the national system is about.

INT. Yes. Understood. Right. Okay, I don't think I have anything else now. I'd like to reserve the right to send you an e-mail, if needed, in the future.

RESP. Yes, yes.

INT. I don't know if you have anything else to add.

RESP. [Overtalking]. Good.

INT. Good. Thanks very much [name].

RESP. I hope it was helpful.

INT. It was, it was really helpful, thank you. Right.

RESP. Good, no. Bye.

INT. Bye-bye. ⏱01:00:27

B.2 Belgium

RESP. Two minutes ago and that does not mean I catch up in all my mail boxes and all my meetings. ⏱00:00:00

INT. That's fine. I was just wondering if there was a problem with our email server here.

RESP. They do come through. They do come through.

INT. Are you ready?

RESP. Yes. Thank you for sending me the questions upfront. I glanced at them and I had no immediate real problems. So let me just open the questions. But you can fire… I got a presentation that starts at 4:00, so I have to stop a couple of minutes to 4:00 at the latest.

INT. Sure. Well, the questions are general for any eID system. But since for their deliverable, we're focusing on Germany, Austria and the UK, I would like us to focus more on eID systems in eIDAS rather than specifically to the Belgian one. If that's all right? ⏱00:01:22

RESP. Well, let's try. There is no eIDAS identity system and there are only the Member States' solutions.

INT. I mean more in a hypothetical scenario how the Belgian system would interact inside the eIDAS framework, so the minimum data sets, the unique identifier, that kind of thing and in terms of privacy.

RESP. That's okay. Can you see my video? Does that work or is it off or?

INT. It's off at the moment.

RESP. So how do I turn that on? I found the button. So let's see. Not perfect but good.

INT. We're talking about the Belgian system and would you be able to give a quick overview of it?

RESP. Yes, the Belgian current system is essentially a smart card with data files which contain identity information like name and address and gender and national identity number in the file system. And then it has two key pairs and an authentication and a signature applet orbit. That in a nutshell, is the Belgian eID card.

00:02:54 INT. And is it only for public services or is it both for public and private Service Providers?

RESP. It's for both. It's your identity cards, it's your travel documents and it can be used to do electronic authentication and signature for anybody that cares to rely on the outcome of authentication or a signature.

INT. And in the electronic identification or authentication, are all the attributes that you mentioned before transmitted?

RESP. Well, I think that depends. The underlying thing is the crypto challenge-response, but to do the verification, you need to have the certificate. And the certificate contains, I think... I don't know whether all the attributes are in this certificate or you can probably find out very quickly. But it at least contains your national register number, which is the source of any potential privacy violation. This is the Belgian government identity number that you have, the primary number one and it's in the certificate. So that is an extremely bad design, but it's been designed like that.

INT. And if I remember correctly, the format of the ID number contains within your date of birth, correct?

00:04:48 RESP. Yes, your date of birth and I think also your gender it's explained, I think, on the website of the national register. If you want this type of details, I can look into some presentations of the national register or we can go there. If you want to have specifics, that can be arranged. We can look in the specifics now or later.

INT. I think I already have some sources describing the format, so I'll get back to you if I need something additional. So in this case since that is the design, how is the system secured against linkability? Is linkability an easy thing to do in the Belgian system?

RESP. Linkability is technically feasible and legally forbidden.

INT. So legal measures really?

RESP. Yes.

INT. So would you be able to explain shortly what you understand as Privacy by Design or data protection by design in eID system?

RESP. Well, in the Belgian... You mean in the Belgian system or in general?

INT. Both hopefully.

RESP. Well, I'm looking at the questions. How do you understand Privacy by Design in the case of eID systems? Well, the starting points are the IDs from Kavookjian [unclear]. Again, I suppose you are familiar with the IDs from Kavookjian and the website and all of that, right?

INT. Yes. ⏱00:06:42

RESP. So the Belgian eID system is a gross violation of anything that has to do with Privacy by Design. And I was scolded at a couple of times for bringing this up to the director general of the National Register, not the current one, because the eID project was launched, I don't know, like 15 years ago. And he said, but we need to have the national number in the certificate and in the data files because we need it in the applications. If we don't have it in the applications, we have no linkage. And if you then say, but for that purpose, you don't need to have it in the certificate, you can capture it through the protocol. In an exchange, you can ask for it. And then this guy was not really a technical IT guy or whatever. He preferred not to understand that and to say, well, if the certificate is going to be used for identification, we need to have the national number in there. End of the discussion. So also the various academics argued with him that this was not so well thought of, but he is the director general and he decides. And then he, well, made a deal. He implemented it legally with the Privacy Commission that by definition, it is forbidden to use it, but then there would be a series of exemptions where you could use it. And then they made, I think, something like National Implementation Act that allowed the usage of this national ID number in the ID systems for healthcare, social benefits, all of these for all of these systems. Then that's the way it is actually ⏱00:08:48 addressed. So if you are a bank and you have the certificate of [name] and you have the national identity number of [name] from the certificate, it is forbidden that you store it. It's forbidden that you use it. You will get it... You will store it because to verify an authentication online or to verify a signature. You need the certificate. The certificate contains the national number. So this is a kind of, technically, insane way of handling it. But then legally, you should then throw away the certificate after you have done the verification or something. This is total mismatch between technical reality and legal implementation.

INT. I will come back to the legal measures when we discuss eIDAS in a bit. But so you said the linkability before is technically possible, are any data minimisation measures implemented in the system? The way you understand data minimisation.

RESP. Depends what is the scope of the system. The eID system consists of, let's say, the ⏱00:10:03 card, the token and then the token is linked to a person somewhere in a database, that's the National Register database. And then there are the services that allow you to do a verification. There is the federal authentication server and there is an OCSP responder. So the normal definition of what is the Belgian eID system would probably be it is the database and all the transactions that form the national eID system, let's say on a central computer system. Then you have the enrolment mechanism through all the [unclear], where you do the proofing. And then you have the citizen who has his eID card. And then there is a federal authentication server that you can, if you're a company or a website, you can rely on to do authentication verifications. And then there is an OCSP, online certificate status

protocol resolver, to verify that certificates for electronic signature are still valid.
So that's probably a reasonable definition of what is the eID system. How is data
minimisation implemented within that system? I know there is a lot of access
control on the content of the database and that's good. But it's an old-school
relational database with the basic data mobile, which is fine grained and then there
is access control. So data minimisation in the sense of is it the minimum data set?
⏱00:12:13 Is it really the... Have we thought about not storing something because we don't
really need it? No. This is the system that is 30 or 35 years old so there is no, as
far as I know, there is no real notion of data minimisation applied.

INT. So I'm going to skip, I think, all the questions about the persistent identifiers and pseudonyms because you've answered already.

RESP. There is a persistent identifier in user national number.

INT. So in a potential scenario where the Belgian system is notified in the commission and starts working with eIDAS then, does the way it's implemented, does it pose risks in terms of linkability in other countries? Because if... What I'm trying to say is you've got legal measures in Belgium to compensate for the technical capability of linking records, but those legal measures cannot be imposed in foreign Member States. Therefore do you think that creates a problem?

RESP. Well, I hope not because at European level, we have GDPR. So if you are a Spanish Service Provider and you want to rely on the Belgian eID, well, through the eIDAS note, you only get the minimum data set. Because that's what's exchanged through the eIDAS note, and so the national number is not part of the eIDAS minimum data set. And then you will get GDPR rules on what you can do with that data that you get when you process it there in Spain.

⏱00:14:17 INT. If the national ID number is not part of the minimum data set, what would be used instead for a persistent unique identifier?

RESP. Well, what is the system in this case?

INT. So the Belgian system, we said there's a national ID number in it that I'm guessing is used as a unique identifier, as a persistent identifier?

RESP. That's correct.

INT. So in terms of the minimum data set of eIDAS, which also requires a persistent unique identifier, are they going to use that same ID number or are they going to change [overtalking]?

RESP. That would surprise me and it would even surprise me that eIDAS minimum data set doesn't have... I don't know it by heart. Let me check. In what act is that defined, the minimum data set?

INT. So Implementing Act 2015/1501 or it might be...

RESP. 1501?

INT. I think it's 1501. It might be 1502. Let me…

RESP. One of these. Just a second. 00:15:35

INT. So 1501 in the annex and I can read you what it says, if you want.

RESP. I'm opening it now. In the annex?

INT. Yes, annex.

RESP. The minimum data set for a natural person, family name, first name, date of birth, a unique identifier constructed by the sending member in accordance with the technical specification, which is as persistent as possible in time. So you're right. There is a persistent identifier. Well, I've not yet seen… There is not yet a Belgian publically-available implementation, but my educated guess would be that they would use this, the national number.

INT. In which case therefore, do you think that that might pose privacy risks?

RESP. It would be used there unless they cook up another identifier, which is where you will then guarantee to be unique and consistent and persistent for all usage across eIDAS. But I think we just need a couple of moments to find that out .

INT. Just to put it in context, I don't know if you're familiar with Germany's notification, of their system?

RESP. Somewhat.

INT. So in summary, they are proposed… I'm guessing you already know that the German system has pseudonyms instead of persistent identifiers? 00:17:36

RESP. Yes, like the Austrians and so on.

INT. Exactly. So when they notify to the European commission, they said that every Member State is going to receive the same identifier… So they're going to have one identifier per Member State. So all public services in Belgium are going to receive the same identifier instead of receiving different identifiers per sector and only private services will be able to reque… Well, they're going to get different identifiers per private service. So this is, I'm guessing, because the identifier per Member State is going to be free, whereas the private services will have to pay the German ministry to get a certificate. But in a scenario like that, do you think that endangers the privacy measures that can be implemented in the German system? So that that, does it bring privacy down, participation in eIDAS? Is basically what I'm asking.

RESP. I'm not sure I understand what you're asking. You just explained to me that the Germans have a much better system that includes pseudonyms, which the Belgians don't have. What is your question?

INT. So the German system is able to change the pseudonym according to use, but used in their cross-border setting is going to transmit the same pseudonym for the entire 00:19:18

foreign Member State. Therefore in practice, it might be looked at as being used as a unique identifier, as a system unique identifier much like the Belgian identifier.

RESP. So it's going to be a pseudonym which is one-on-one, matching with the natural person. One natural person will always have the same pseudonym.

INT. For every public service of a certain foreign Member State?

RESP. Yes. And it might be another member in another Member State. But over time, you could build up knowledge of the German guy, for example, interacting with Belgium, because he would always be using the same pseudonym.

INT. Or the Belgian police is going to know that the Belgian Tax Authority is interacting with the same guy because both are receiving the same identifier per se.

RESP. And now, what is the question?

INT. So if the Belgian system is notified in the same fashion, using the same identifier group Member States, do you think that entails privacy risks?

🕐00:20:49 RESP. Yes. The current system of having only one persistent identifier within Belgium is having a lot of privacy risks. And if you would use that to reach out to the 27 other Member States, that would only make things worse. Now, because you can do more linkage... I must tell you there has been a new RFP, I think, either announced or issued for the next generation of the eID card. But that might actually also impact the whole system and the database in their transactions. And I'm meeting the guy who is in the Ministry of the Interior, responsible for the eID system. And I'm lunching with him somewhere in January, second half of January normally, because he wanted to explain a bit where they are going. It is perfectly possible. This is a closed RFP. That in this RFP, the government asked for a system that can generate pseudonyms because they feel that the importance thereof has been increased with things like the GDPR and so on.

INT. So in a case of...

RESP. It might be. I don't know. I have not yet seen. I can check whether I have it somewhere on my PC or something, but I've definitely not read the new RFP for the Belgian eID.

INT. That's fine. But in a hypothetical scenario where this is the system you're going for, do you think the way eIDAS is being implemented can support pseudonyms? Are there any limitations in the way pseudonyms can work inside eIDAS [unclear]?

🕐00:22:55 RESP. The strength of... Pseudonyms are limited by how can you link them? And if you have the three other attributes, family name or names, first name or names and date of birth, this set of three attributes together can promptly give you quite some linkability. So you can have a brilliantly specified unique identifier persistent as possible in time, which is a pseudonym, but then the results that if you try to link queries. And even if you only use first name, last name, date of birth, you could probably already do a lot in terms of identifying a very small set of people that match that set of attributes. And there, the legal defence is probably your best defence now, because the minimum data set, that's been agreed. That's what they're going to be exchanging.

INT. But so in terms of technical measures, would you think selective disclosure could be a way to resolve that?

RESP. Yes, if you would implement selective disclosure things at an EU scale.

INT. Are there any other technical measures you can implement too?

RESP. Well, I think there are two main lines of thought, two or three main lines of thought. You used the term selective disclosure but underneath it, there are a couple of underlying IDs. One is the family of solutions from a guy called Stephen Brent [unclear], another one is coming from Camenisch and there might be a third one. And people invent new stuff all the time. So if you would come up with a selective disclosure system, a la Stephen Brent or a la Jan Camenisch, done for privacy across the EU, that would probably be a very good ID. But it's expensive and you need to pick one and somebody like the commission would then have to drive it. And apparently right now when you look at eIDAS, they are not driving it that way. They are rather driving eIDAS in the direction of using electronic identification for anti-money laundering. And if you want to do anti-money laundering, you're the opposite of pseudonyms. You want to know who this person is. ⏱00:24:37

INT. But at the same time, they're also trying to involve private sector into cross-border eID. So they're currently in Facebook, for example, to use eIDAS. So would you say that in that case, that...? But we need more privacy if the private sector is going to be involved?

RESP. Well, I think there is not a simple fixed answer in the sense that in the case of banks using eIDAS for anti-money laundering, they want less privacy. In the case of shopping, e-commerce, you may want more privacy, but that's just because the use cases are very different.

INT. So wouldn't the system that allows for different attributes to be transmitted depending on the use case, wouldn't that be preferable? ⏱00:27:17

RESP. Yes, absolutely. The challenge is that there are many different use cases because there are many industry segments and within each industry segment, there are a multitude of use cases. But ideally, if you have enough time and a bunch of smart people, you can probably cook up some scheme for what type of use cases per industry would then be best served by something like the eIDAS minimum data set which can then be used for anti-money laundering. And other use cases where you would have selective disclosure style protocols because that's good enough for that use case. But then you would probably end up with building a sliding scale with perfect privacy on the left and no privacy on the right. And you would have then to... And you would position your use case somewhere along that scale. But it will be, I think, a very long scale and I've never seen any project or any research that actually tries to build that scale. Maybe you have, but I haven't.

INT. No, I'm just trying to figure out if there is a case to be made that we need in the future to think more about technical measures to accompany legal measures. So in other words, are legal measures enough to protect us as they are or do we need to add technical measures as well?

00:29:18 RESP. Well, I think with what I have learnt over the years is that you need both because I've seen banks where they do data mining and they use the Belgian national identity number . It's so convenient and, well, if they have an audit, they will then probably make the data set disappear or convince the auditor that they don't do it or they don't have that data. But they tell me, listen. For us, this is very important to be able to link people to one another, to build family trees because then, we know where the money is and we know what type of product we can sell where. So even though it's perfect, what they do is completely illegal in Belgian. There is a legislation that says you cannot do this. Still, they do it. So the best protection we can get is from the combination of legal and technical measures. And I'm not a lawyer, so I don't have much to add there, I think, to what you can do on the legal side. But on the technical side, then I think one thing would be to come up with this sliding scale with zero privacy on one hand, perfect privacy on the other hand, map the use cases on there. And then for every use case, have both the technical and the legal measures. But that's maybe a horizon toward a dirty project or something to cook up. I don't know of anybody who's actually doing this, maybe commission is doing it. But maybe Sutton [unclear] is doing it. But it would be nice. It could be a nice thing.

00:31:09 INT. Well, the first problem I can see with legal measures is the commission can't actually force legal measures to Member States.

RESP. What do you mean? They write regulations and they are enforced on the Member States because they go through parliament. And once they've been through parliament, this is the law enforced onto the Member States.

INT. But for example it would be very difficult, I think, for the commission to say that because in Austria, for example, they've got 40 sectors that are not allowed to share data with each other. Therefore in the UK, the public sectors would not be able to share data with each other. Do you understand [overtalking]?

RESP. Yes, in that way, it will not be possible. They have to come up with a consensus on all and all the Member States. Fine, it's acceptable and that could be looking ten years in the future, for example, that we will have a technical regulation. Because in some areas, they publish things that they call RTS, is a regulatory technical standards which define the technical stuff under the regulation. And there, they can prescribe protocols and things like data. So they could, but the model that

they would have to enforce would be, they need to have consensus in the parliament that this is doable. And in the long run, I think it's probably where we would go, but we're years from that because implementing things like the Camenisch or the Stephen Brent's things are complicated and expensive. The Germans and the Austrians have a very basic childish almost implementation. The Dutch, they 00:33:12
started with the national pseudonym scheme designed by Eric Verheul, a Dutch researcher. And I did due diligence on it in the course of this year. And when I connected a couple of weeks ago with somebody from the Dutch Ministry of the Interior, they said but they scrapped it. It's technically, mathematically maybe good. But it's so expensive that they will focus the budget now on having a good national eID solution and eIDAS support and that's where the money is going today. And that they have original budget allocations for a national polymorph pseudonym solution. There's really cool stuff, but it will be very, very expensive and not proven. So they decided, well, from a privacy point of view, they will be brilliant. However, let's first walk before we try to run. We can't walk today, so let's first walk and then ten years from here, let's maybe try to run.

INT. Well…

RESP. And I don't… You have the German and Austrians. Are there any other countries that having pseudonym solutions?

INT. I think Portugal is developing a system that is similar to Germany's, off the top of 00:34:35
my head. And I think Italy and Spain are looking to change the way their systems operate because up until now, they were operating with unique identifiers, and now the one [unclear] beef up their privacy. But as far as I know, Germany and Austria are the most privacy friendly.

RESP. Absolutely.

INT. Well, I'm going to have an interview with the Netherlands at some point, so I might ask them about what you just said.

RESP. Well, they had a scheme called polymorph pseudonyms invented by Verheul. I can send you the academic description of it because this guy is a researcher and well, he's involved in the Dutch eID for a long time. And he said, well, you should have something which is more privacy-minded, so let me cook up something for you. Well, here it is and then they initially liked it and then realised how much it would cost. But his design is in the public domain. I can send you the paper if you're interested.

INT. I can probably find it. If not, I'll ask you for it. Well, at this point, I'll probably let you go because you have your meeting to go to. Unless you have anything else you want to add before we…?

RESP. No, I think this is very interesting and I hope in the long term, it's going to give 00:36:09
us a European eIDAS file system which is more respectful for privacy, so great

work that you are doing there and that you are thinking about this. And this is in the context of one of the deliverables like three point eight or something or?

INT. Two point eight.

RESP. Two point eight, that's it. So I look forward to reading that.

INT. Thanks very much.

RESP. I hope it was helpful.

INT. It was. It really was. Thanks for your time.

RESP. Bye.

INT. Bye.

00:37:01 RESP. Bye.

B.3 Estonia

00:00:26 INT. Mind if I record this?

RESP. I don't mind, it's okay.

INT. Brilliant.

RESP. It will be easier for you to fill in the [inaudible] later, that's something [inaudible].

INT. Yes, go ahead.

RESP. Okay, and for the beginning, to understand Estonian eID is that everything actually started in there somewhere in the mid or second half of the '90s. We didn't have any legacy, as many other countries because the country was just gaining independence in the beginning of '90s. And all the Soviet systems was basically trashed and regulations was also, everything was started from scratch. So in Estonia we were also really, really concerned about the privacy questions, we 00:01:26 didn't want to have this Big Brother effect in one hand. On the other hand, we didn't have this issue in our society either because, well, to be honest, people has been in decades of ruling of other countries or nations or on the Soviet so people were used that you have all this Big Brother. People were used that you can talk openly and so on. So it wasn't an issue that the government is a Big Brother, people were used to it, kind of. But when they took out our concept for Estonian eID, actually it was an ID card. The question was that we need to have some unique identification document because the passport has several disadvantages. First, it's a paper booklet, so it's lots of papers in it and you can easily damage it and then it's not valid. Also it's an uncomfortable format to have it in the pocket and not all the people have passport because passport is usually taken as a travel document, actually. So and also the driving licence, not all the people have driving licence. And we had groups of people who had no identity document, so we really

were eager to start to issue identity documents that are, let's say, secure, not so not easy to falsify. And it has to be in a plastic format to last for a long time and it has to be in the credit card size to fit in the wallet and so and so on. So this was [unclear] so many countries was doing that in the '90s actually. Many, many countries around the world took national identity documents in the credit card form. The next thing was that should it be open for the future? And here Estonian 00:03:31
government was also co-working with some private sector companies to research what is the future trends. Also with the Estonian scientists and the universities, what would be possible to implement today that is a future save. And then we came out that the technology that has been existing for almost 30 years there, the smartcards, has been developed for a later ten... Let's say in the second half of the '90s, the smartcards was being developed a lot, so they had a lot of new features, a lot of new things. And when we're talking about electronic society, then it's much more convenient to have also eID together with an ID. There was several reasons actually, the base reason was why we started to build our e-societies because we're a small country, we have just 1.3 million inhabitants as a population, it means that... And the people gets older and older, it's a demographical problem, as every country has. And the density, in Estonia the density of population is really, really low. So some places you have several kilometres between the houses and it means that we do not have enough people to serve people from the governmental perspective. So we need to automate as much as possible and make all the services available online, 00:05:22
if it's possible. So with that case the people who are living in rural areas, they have access to the services, at the same time the government doesn't need to have a huge budget that goes only to the civil servants, payment for civil servants. So this was the issues what was the triggers to start to build e-society. But going back to our eID, the eID cards we start to issue 2002, it was national identity physical document with a chip on it. The basic idea was default enable, what we saw, why we did it, we looked what other countries is doing. We didn't invent anything new, we actually copied best practice and if we saw that somebody made some mistake, we tried to avoid that. Many countries issuing eIDs default disabled. The only reason... What I understand, it's my personal opinion now. What I understand is because lack of knowledge about security and privacy. So just in case, let's make it disabled is the reason. For us it was vice versa, if there is a risk there should be a mechanism or with just a few minutes disable it, but by default enable. Because if you give it as disabled, it will be really few people who will start to enable and use it and then you don't get this critical mass, then you don't get the good services. And it's always as an egg and chicken question, if you don't have customers, you don't get the service. If you don't get the service, then you don't get the customers. So you have to kind of force people to get this critical mass. So we started to issue, 00:07:35
so for the first year I think it was kind of 200 000 cards was issued. But within three years almost all population was covered. Of course these cards is mandatory

from 15-years-old people, if you are below 15 it's not mandatory to have. But today, I looked at statistics, we have 1.35 million people, but 1.31 million eIDs in circulation. Why we have for the kids? Well, this card is also valid as a travel document within EU. And it's much more easier for parents to prove or to have kids' identity data with them if their parents have kids' ID cards in their wallet. It's much easier too and hassle-free, so usually when kids born, then after the first visit to some officials, people taking the ID cards you have for kids. But it means that it's also default enabled, it means that if somebody gives this, or a kid itself, gives signature, let's say, qualified electronic signature with this card, it will... It depends on the context, but usually it will be invalid because he is underage. But it's context-based because kids can have let's say polls in the school or class voting, for example. But it's really rarely used by the kids, it's usually when they get, like, 16, 17, then they start to use it actually, electronically, more. For accessing portals, yes, it is used, for example e-school. Some kids, not many kids, because kids are more password-minded and they are kind of not so developed in their mindset yet. So really few kids are using their cards as electronical access, but the physical card
00:09:54 they have. By default enabled, it means that if you are the person who really has issues with the government and you don't like that, you can always call 24–7 phone number and suspend your certificate so nobody can use it electronically anymore. And even if you are, let's say, if you're really, really a geeky person, you don't like... And you are suspect in that everything is... The Big Brother is everywhere, you can always take a screwdriver and mess with this chip, the possibility is always there. But the physical document is mandatory, actually, to have one physical document. So let's go further, what's on the chip? So chip is simple SCD, we decided that this, for authentication and signing, it should be on the sole control of the person. So it means that the person has the chip where the private key is on and also those private keys are generated in the chip. So in the manufacturing, when the manufacturer of the cards, there's no, like, a super server which generates keys and just writes them on the cards. No, the card gets instruction to generate a new pair of keys and the card gives out just the public key, the private key is stored in the secure module. And this has been used previously as well, we had this functionality to regenerate, basically if you suspect that maybe government or somebody has regenerating... If you are technically aware person, then you can check the protocols and everything and you can suspend your certificates and you
00:11:55 can apply for a new certificate. And then you can check that, what's happening with the card in your computer, in your software, what kind of transfer packages goes in and out, what is the protocol. You can see that actually there [unclear] instruction goes into the card, card asks your PIN code because it's protected by the PIN code to access those functions. All the functions that use the keys are protected with the PIN codes. And then you can see that only the public key goes out and it goes to the certification authority, which generates the certificate to this.

So technically it's a secure signature creation device and we're using two pair of keys. Some countries, like Greece for example, I suspect you [inaudible].

INT. Yes, I am.

RESP. You are using only one pair of key so you can sign and authenticate with the one certificate, am I correct?

INT. Yes, we don't actually use it yet, but yes, that's the plan.

RESP. Because in 2010 or '11 it was when you introduced your ID card and then I remembered this concept. And why we are a little bit against that, it's really easy to confuse the user if you require the same PIN code, because PIN code is related to the key to the certificate. Person doesn't know if he logs in somewhere or signing something, but juridically it's completely different consequences. You log in somewhere, it's not your free will, you are giving. But when you're signing 00:13:38 something you're taking responsibility and that's why we're keeping separate those two things. It has to be one certificate and key with a PIN code for login and one for signatures, completely different PIN code and key. So this is the basic of the technology, how does this, our ID card, works. And when we're talking about the login somewhere, then the regular SSL authentication is done, it's supportive natively by our web service. And the only thing is that webserver has to be configured that it will not generate keys for the customer's computer, but it will use the keys that customer sends from his ID card, his certificate. So basically it will be authentication with not server certificate, but authentication with your personal certificate that is generated through your ID card. And then the question when we're coming more and more to the privacy question. The model we use is also known as a KISS model, keep it simple and stupid. The thing is that the less data you store somewhere, the less hassle you have to protect it. So in this case an Estonian ID card, the only personal data we store on a certificate is first name, last name and unique identifier.

INT. Now is a unique... As far as I understand your unique identifier is your national 00:15:30 number?

RESP. ID code. Okay, I will take a separate topic right now about identifier, to explain what it is. The identifier, it is consisting of 11 numbers and it is generated when the person is born or when somebody moves to the country and starts to live here. But the idea is that everybody who lives here permanently have identity code and this code is unique and lasts for a lifetime. It can be changed only for two reasons, one is the witness protection and the second is if you change your sex. Because this number is not impersonalised, this number consists of some personal data. It consist of which century and if you are a male or female then it has also your birthdate and then there are other numbers, control numbers that makes it unique. So in our Estonian case it was for decades been discussion, why we have such ID code, why we can't have, like, a random number or something? The reason is historical, before 2000 and even in the early ’90s, we started to... Early ’90s we started to issue these numbers to the people. The numbers was generated by the hospitals and in those days we didn’t have Internet everywhere, even intranet was unusual. And the system need to be... The system was built that... Or not the system, but the algorithm is built that every instance who is generating numbers can generate a number without colliding with other entities generating number. So 00:17:54 those last numbers actually is a hospital number and the number of baby born in this day and then a control number. Additional control number, it’s like a CRC or something, control number that in case there are some matches. And this gives this unique possibility that you can generate those offline and be sure that nobody else has been generating or taking up the same number. And since then all the information systems, all the governmental... And not only governmental, but in the private sector as well, all the data bases, all the infrastructure is built to knowing that algorithm. It means that there are no system that’s asking you separately, give me your birth day because it is extracted from your identity code. And because of that, knowing someone’s birthdate and name or even ID code cannot be accepted to be as a primary key somewhere. It means that this data, when you build some information system or some kind of procedures, this data must be considered as a public data. So knowing this data cannot be compromised or made identity fraud and that’s why we’re living hassle-free here with the... So basically if someone knows my name, my birthdate and even my ID code, he cannot take over any data about myself. And this is the reason why these kind of data is also stored on a certificate. So you have birthday date embedded in the identity code and you have 00:20:02 the first and last name. And knowing this data, you cannot access anywhere. So to access you have to have those ID cards, you have to log in and know your PIN code, have active certificates and so on. And when we’re talking about KISS model, in KISS model it means that we only identify physical person, we never accredit them, we never authorise him, we never give roles or anything. Authentication is just identifying physical person. So when the question is about the roles, that if I am a representative, if I want to go and have a service for my company, I’m owner. Well, all the data, rows, authorisations came from different registry data bases. So when I log in for example to citizen portal, the citizen portal automatically checks all the registers, population registry, military registry, business registry. All the registries and collecting all the data that government has about me and show me in the one page. And this is one thing that we call for privacy by transparency. The person has right to know what kind of data government has about him and also, if the person sees that some data is incorrect, he has to be able to correct it. So in our case, you don’t get access if you don’t have access and we had also in early days a discussion about why the heck we are not issuing a role base certificates? Well, there is a simple answer for that. Let’s say you have role based certificate and 00:22:06 issued to your document, which is your personal identity document. And now let’s

say you have rights for money transactions in the name of company or something,
you are major financial officer or someone. And now you will get fired, so what
can company do to prevent you to misuse your power? If it's in the certificates
only you can revoke or if somebody else revokes in your name, then the procedure
takes several days until it will be accomplished. You can transfer money and do
anything you want, but if the rights and roles came from the databases, then the
owner of the database is just changing one record and that's done. In this case
the company will just delete your certificate and your permissions in the database,
that's it. So this gives kind of better control for the business as well.

INT. Would you say that that data being public knowledge makes it so that there's no
issue of... There's no problem against linkability? Because I'm guessing since it's...

RESP. No, exactly. This is another... Actually it's not eID related, but this was when
we started to develop our eID the first thoughts and ideas in 1999. At the same
time we started to build platform, we call it X-Road, if you have maybe in the
Internet you can find some information about it. But what it is, it's a platform, it's
actually a set of protocols, technical protocols, to interconnect different databases.
So what we're doing is we have some adaptor servers, security so we don't have
any super database in the country. We kept status quo as it was in the mid of the ⏱00:24:15
'90s, that every institution, every company, every municipality, they have their own
database, they have their own system and everybody maintains their own. And
everybody is owner of their own data so the only thing we had a struggle with
was that how we can exchange this data and also interpret the one-only principle.
Because once-only was a big issue in the '90s and we wanted to get rid of that.
The problem that people have every time they go in different portals they have
to give up the saved data, I mean come on, government has this data. So we
created this in the end of the '90s and in 2001 or 2000 it was started to use, it was
X-Road that interconnects all public sector databases. And the control, there are
strict rules that are also conformant with the GDPR, who can ask what kind of
data and what they have. So if you open access to another database to request...
Let's say a simple example, if we have a population registry that collects all the
data about the person, there is a person, his living address, his first place, also
relations to his parents, to his kids and wife and so on. And then we have a driving
licence registry for example, and now how we can interconnect those two registries.
Well, the owner of driving licence registry has to give his certificate to population ⏱00:26:00
registry owner and say that, please, give me an access, I need to have an access to
such records. And this is an application form he fills in and also in the form he
has to point to the laws and regulations that gives him the power to work with
this kind of data. So in case the driving licence authority who is taking care of
driving licence registry doesn't have legal right to request person's, let's say, his
living address. Then the population registry will reject to give them an access, but
if they have legal ground for that, their population registry well open this query

for them. So this database can always make the queries about the person's living address to the population registry. And this is overseen by our data protection [overtalking] they have several auditors who is going through every year, all the databases. And to see it more transparent we have also a catalogue of all databases and data which is publicly available, but it's unfortunately in Estonia only. If you are interested about those links actually, after our interview send me an email, because I will forget because I will deal with that Monday. With all links you want to know, I can send to you. Like RIHA is an information system that categorise... It's like a phone book, it's like a huge phone book with all kind of institutions where databases connected to different regulations. What kind of regulations they have, on what ground they have created this database, how they're interconnected to other databases, what kind of data they share with other databases. So this 00:28:20 kind of catalogue we have and you can also visualise it. So you get like dots and lines between them, so you can see directly and this is also publicly available. So this is another measure for transparency, people have a right to know. And also, if I am an entrepreneur, I start a new service and I want my database interconnected to some other data because I don't want to collect from the people maybe, let's say, their home addresses or whatever. I don't want to collect from them if they have a driving licence or not, I want to ask the registry of driving licences if this... I don't want to know driving licence number or anything, I want to know just if this person has right to drive, like in B category, a simple question. So I need to know who is responsible for this database and what kind of queries I can do against it, towards this database. And there I go to this catalogue system and checking from there.

INT. So from what you're saying, and from what I understand, this is all policy-based, right? So it's based on having policies that forbid you from accessing certain databases?

RESP. Absolutely. Certain databases are publicly available and they have been questioned that can we have it as a public data, in principle why we need to have it in separate databases or so on. Some databases have really strict rules, like health records, they are really the... Health record and population register, those are most controlled databases and there are a lot of strict rules and regulations around them, who, 00:30:17 on what behalf and how? But me, as a person, I have always right to know all the data about me. For example, if I am as a person logging into the e-health system, website, I can see all the history, all the data about me and my health. If I have underage kids I have a right to see their health records as well, but when they become 18 I can't see. And also if there are, for example, by the court I have been... My parental rights have been reduced, so I can't see either. But all the other doctors, they can't see my records, only specialist who are appointed to... Let's say I get sick, I go to the doctor, my house doctor can see my data, but me as a person, I can always tick which data I don't want them to see. And also tick if I want that no doctor will see without my permission, my data. I have full control about it, me as a person, but in general, if I don't tick anything in, doctors get access to my medical records when they are connected to the case. In case I get sick, the new case will be opened and doctors who are connected to this case, they will see my medical records. Usually they see everything that has to do with this case, but some basic records as well, like if I have allergies and these kind of things. So this is something we are really concerned about when our governmental 00:31:53 or private sector doing a new business, starting a new databases, starting collecting data or sharing data. We are really, really concerned about it that there has to be rules, there has to be some supervision because the privacy is actually number one. Even if it doesn't sound like that, that we share the numbers and everything to the people. That we have kind of, government gathered kind of statistics to see what kind of people's group is using what kind of services more or less and these kind of things. But this statistics is possible only thanks to this kind of personalised [overtalking].

INT. Yes, understood. My only question is, if privacy is solely policy-based, in a hypothetical scenario where you join eIDAS in the future so you're exchanging data with other member states. The problem then becomes you can't really control the policies that other member states have. So wouldn't you say that in that case you would need something technical to enforce policy?

RESP. Usually it's a sector-specific. We can take it as example in taxation, there is 00:33:16 already many, many countries making tax authorities exchanging the data. Then the question is, what Estonian government or Estonian law says? If Estonian law actually doesn't prohibit and allows to exchange certain data, for example person's income or paid taxes, with other countries. Then it is doable when tax authority have this bilateral agreement. For example we have it with Finland, with Sweden, with our neighbour countries, we have. So it's to prevent double taxation when the person is living in one country, working in another country so if another country takes taxes so home country doesn't take taxes again, so for this kind of reason. And this is bilateral and in the bilateral agreement there are also described all the responsibilities and these kind of things. And then we're talking about the sector-specific, I don't see it as so big problem. The bigger problem might be even not from the Estonian side, but from the other countries who many countries, like in the UK, there are some strict rules for certain databases. It's just one statement, it's prohibited to send abroad this kind of data to use outside of the country. So if one country has this kind of laws, then they have a problem. And today we do not have a... When we're talking about public services and social services, then we do not have any such a specific restriction. Yes, we have restrictions that who can access to the database, but not what kind of data can be sent out. Access to the database or sending data is a different meaning, different things actually.

00:35:37 INT. Would you say it makes a difference if the service that requests access is public or private?

RESP. In our case for private... For public sector we have older regulations, for private sector we usually, private sector to get from the public sector's databases, they have to first go to the X-Road. But to get access to the public government-owned X-Road because private sector has their own. But by the public sector X-Road then there are strict regulations, it means that also they have to... Their system will be audited by the government annually. If the private sector is okay, like telecom and banks, they are okay. Actually, not the government who is auditing, but government has setup of the audit's rules that they have to submit annual audit reports to us. So we know that their system is okay, that there's some third party independent auditor who has qualification, has been auditing and checking that they are not misusing with the data protection and privacy and these kind of things. And then they're giving them access, yes, if they have legal grounds.
00:36:59 For population registries, for example many, many private sector actors want to have access to population registry to make enquiries to population registry. But it's so strict, so we have only few, it's like if you're a vital Service Provider, if it's like a gas, electricity, communications like phones, banking, those are vital services. If you're a vital Service Provider, even if you are private sector, then you get automatic access because by the regulation you not only have right to have access, but you are obligated to check whether the information you have is up to date of the person's living address and so on.

INT. So would you say in any eIDAS settings, and I'm assuming you're familiar with the eIDAS?

RESP. Yes, absolutely, this is one of my jobs actually, one of my task on a daily basis.

INT. Brilliant, so in the eIDAS setting, would you say then that Privacy by Design is no issue?

RESP. No, in our case we don't see it as an issue, for us. Because we have the whole framework of rules and regulations for that, we're aligning our regulation right now with the newest GDPR, we have basically... Yes, well this is a new one that every country has to do that. Also overseeing all our framework, that if it needs to be updated. In our case the data we use for authentication in terms of eIDAS, this data is concerned more or less. It's not anywhere written that it's public data, but
00:38:58 it's handled as it should be handled as a public data. So it's strictly prohibited to use this data as an access or permission to other personal data. So and in eIDAS context right now we are accomplishing our assessment of our eIDs, actually the government has issued six different eID tokens, five of them are smartcards. We have besides this ID card I described, we have exactly the same chip, all the smartcards have exactly the same chip and everything. Then why they describe them as a different scheme is because we have a different issuing process. And ID

card is what we're talking about the most, but then we have a digital ID, it's same thing as ID card, but it's not a physical document it's just for digital use only. And this is, for example I use one, I have one in my office desk in case I forget my wallet at home or I lose my wallet. I can continue job, I need to have a card, so I always have one in my work desk, just in case. It's an additional, it's like in the physical world, if you think that you have an ID card, then you have a driving licence, then you have a passport. They're all valid identity documents, they are just different form, but they are connected to the one person.

INT. I expect it's the same that we can get it if we apply for your e-residency?

RESP. Absolutely. And you get then registered in the Estonia population registry as 00:40:33 a non-resident, but registered in Estonia, non-resident of Estonia registered in Estonia, you get Estonian ID codes and through that you get access to the services. Because when you're logging in then the services will check other registries with your data, if you have any data. So here is this regarded as one scheme because the issuing process is different. Then we have also... What was the third? Jesus, I start to forget. One was ID card, then key residence card, then we have resident's permit card. This is regulated by EU, it's a resident's permit card, it's a pink card, you have maybe seen, pink plastic identity documents some people have?

INT. Yes.

RESP. It's people who are non-EU residents, non-EU citizens, but they are living in the EU. So for those cards we are putting also the same chip as an ID card, everything is technically the same, the only thing is that the issuing process is different of the card. And then we have also the fifth is the diplomatic card, it's for people of other countries' embassy's workers who is permanently living... Who is living here for, like, three, four years and they need to have also access because they're using our healthcare system and so on. So these are the five smartcard-based tokens. And then we have sim card-based token, it's a mobile ID. And sim card-based token, the only thing that's different, to explain it as easy... To not go too deeply into the technical, to explain how it works, it's the same thing as ID card, but if you imagine that you are cutting the chip out from your ID card in the format of sim card. So the private keys are stored there, it's not a regular sim card of course, it's 00:42:46 a dual application, it has both the regular cell phone operator sim card and also it has eID part. The thing is that mobile phone is a card reader, sim card is a card and we're using SMS, encrypted SMS, service as a wire between the computer and card reader, as simple as it is. So everything that is technically related there is of course you cannot do it without Service Providers because you need to have a mobile...

INT. Operator.

RESP. Service and so on, but the concept is the same as ID card.

INT. Yes, I believe they're doing the same in Belgium, if I remember correctly.

RESP. Yes.

INT. So you mentioned privacy of the GDPR and this is the reason why we started these interviews basically. Because the GDPR demands data privacy by design, so we're trying to figure out how eID experts understand what that means?

00:44:02 RESP. Well, it means that unauthorised... For me it's really, I don't go deeply into the GDPR's different requirements, I will just take as a concept. In a concept when identifying person the basic data, like let's call it by, like, in eIDAS there are minimum set of data. It can't be handled as private data or protected data because if you handle it like that the cross border authentication will never work. Because you don't know what other side will do with this data and you don't have this control. Even if we have GDPR or we don't have GDPR, it doesn't matter, we're talking about not only public sector, we're talking about the private sector and so on. And if you do not control something then you have to say that this is a public.

INT. So it's a necessary compromise, is what you're saying?

RESP. Absolutely, it's necessary, absolutely necessary. If you build your system that doesn't take this into account then you are in the big trouble. So minimum set of data should be considered as public data or data that cannot be controlled as a private data. Then all additional data... Or one thing, when we're talking about the minimum set of data I mean only the mandatory parts, not the optional parts. The optional part even in Estonia can be handled as...

INT. Private.

RESP. Private, yes. Like living address and these kind of things because living address is more also about relations that you... Who are my kids or what positions I
00:46:01 have in one company or whatever? This is more private, but when we're talking amount minimum set mandatory, it was first name, last name, unique identifier and birthday date, these four things.

INT. I believe the address was amongst those, I believe there were five initially, but I might be wrong right now.

RESP. Well, I think it was four or five, okay. Because initial they also wanted to have, UK wanted to have, also living address, but this was excluded because we were against that, even Germans was against it. So I was in this working group when we were struggling with those implementation acts, so these things should be considered that it's out of your control. So you cannot say that this is deeply protected, private data. Yes, it's private data, but it should be handled as public data because...

INT. So in a scenario where a foreign service requires additional data from the optional data to identify you, wouldn't you say it be better if there was a way that is not relied on the foreign services policy to control which data you actually exchange?

RESP. I would say that it would be better if we have... If you look, eIDAS is a little bit 00:47:35 bigger as a concept not only for identification. eIDAS also describes something that we call e-delivery, so wouldn't it be more... It's my opinion, isn't it more... Doesn't it make more sense if I identify myself by logging in then the system, the counterpart who is allowing me access to their service, they're just checking who I am, not what rights I have. It means that they know that I'm [name], I'm the only... This is the [name] with this identity code, there is no other [name] with this identity code around the world, so we know exactly who this person is, who this person's identity, what is this identity. Now we need to know if he has rights to be represented as a doctor of some hospital or something, then we make through e-delivery a query. Because I identified me with Estonian eID to Estonia doctor registry or whatever service it is. And then this service who has these records about all the doctors of Estonia, first he check who is asking, whether he has a right. And this is again, either bilateral or there will be some other regulation that says if I'm... And then he says yes or no answer, am I doctor or not. And this is what I mean, so identity is not... Let's say identifying person or authentication person is not the same thing as authorisation. And eIDAS-Node concept is made for authentication and this was a big, big fight in our workgroup, I remember for three years ago, just because of this question. Because there was like half of the countries, they 00:49:48 wanted to have eIDAS not only for authentication, but also for authorisation. And half of them said no, no, no, keep those things separately. And the simplest reason is why I think it should be separately kept, GDPR and also security. The more functionalities, the more data you handle, the more problems you will have with the security protection, privacy protection. So this is the reason that keep it simple and stupid, for authentication, use eIDAS, for additional data of authorisation, well, if there are two countries who are okay with that, it's their problem. But from Estonian side, we decided that we will not start to make authorisation system out of eIDAS, so we are just sending minimum set of data. There is a discussion actually, there is one discussion, that should we provide also the data about if the person is representative of private [inaudible]. And why this is in discussion? It's because the EBS, this European Business Registry Service, it doesn't work, it's concept is failure actually. Even if we technically make it work, I have been involved in this project previously, you don't get the fresh data, you don't get up-to-date and usually some proxies are down and it never works. It's always failure, it's 00:51:36 easier to make paper paste query. And there is actually a gap because many, many public sector services are also provided not on the physical person, but also for a legal person. And it has been in discussion, but why are we not implementing it right now in the first stage is simple, there is still a discussion on the standards and on eIDAS expertise level. What kind of representative it should be. There are many countries who's saying that it should be different levels of representation, either I have full rights or I have rights in the manner of singing contracts and so on. And I, or let's say Estonia, and also many other countries, we are against that. For the first in different countries are different semantics. It's the same thing like with the e-health, a nurse in one country have completely different meaning as in another country. Especially when we're talking about access rights, in one country the nurses really, really have access to many, many data. And have a right to make some decisions, in another country have no rights to make a decision. The same thing will be with this business registry, so to be a kind of mid-level access or mid-level rights, what does it mean in one country and another country? Completely different. So me and other countries who are on the same side as me, we are saying that there should only on and off only two statuses, either it doesn't have any rights, or it has full rights. Other way it will never work cross-border, never ever.

INT. Understood.

00:53:49 RESP. Where this question will be solved, it depends on how it will be solved, but if it will be solved, like I said, at full rights or no right at all, then we will open also this attribute to eIDAS to say of the person has full representation right or not, for the company.

INT. Understood. Okay, last one, and this is a theoretical one, from a higher level, from a European level, no matter the architecture of the system. Because I'm guessing yours is centralised from what we talked about, because we talked about interconnected databases, right? So would you say it's more centralised or federated?

RESP. It's federated. The centralised is only platform, the catalogue is centralised. It's like if you think that it's you want to call all data transaction are peer-to-peer, there is no middleman, there is no middle system. It's like if you think that you want to call, like, 30 years ago, you want to call a nice girl. You went to the phone booth, you took a phone catalogue, you searched by the name and the address and, oh, it's probably her number and then you called her. This is what's happening in our case, we have a centralised catalogue to know where you get this kind of data, but then you can call to them, but if they will answer is the question if they trust you.

INT. So thinking of all the possible architectures the eIDAS system have, would you say there are ways, there are techniques to ensure unlinkability?

00:55:47 RESP. What do you mean by unlinkability?

INT. So to ensure that when exchanging data between systems you can't trace where a user is using the eID.

RESP. In Estonian case we can... When we're talking about across border, we can see. We can see... No, actually we can see... Let me think now, we can see which country is using it, but not we can see in detail. Inside in Estonia we can see on base of IP address. Because you see, when authentication is done then the OCSP

request is sent if it's certificate is valid or not. And this request stores from which IP address the request was done, so if it's some web shop, the web shop makes this query and they see the web shop IP address. Of course there is for authentication mechanism there is another option, there is a CRL, so it's a certificate revocation list. And this list you can use without online service, it means that you download this list, you use it for a couple of hours then download new. And we cannot keep and even associate with authentication if somebody downloads this list, and those are impressive, we cannot trace where it has been used. But to protect all these kind of things we have 24–7 service where the person can suspend his certificate just within a couple of minutes. He will call the phone number or email, giving 00:57:33
his personal ID codes, his name and certificates will be suspended. Yes, there is always question if somebody else can do it on other's name? Absolutely, yes. Has it happened? Yes, during 15 years it has happened. For me, for my knowledge it has happened three times. Two of them it was husband was just fighting with the wife and he wanted to mess with her so he...

INT. I'm guessing suspending a card is a very low risk?

RESP. Yes. And we think that it's better to live with this risk that somebody's by mistake closing some others than it will never be closed and will be misused.

INT. Brilliant. Right, so I have I think everything I need. Is there anything else that you would like to add?

RESP. Oh, I can talk about this topic for the whole day. You know what, since it's a Friday and I have a lot of undone job this week I have to accomplish today. So I will continue with my other tasks, but don't hesitate to come back with the questions and if needed we can make additional interview.

INT. Brilliant, thanks very much. Have a good day.

RESP. Bye.

INT. Bye. 00:59:12

B.4 Germany

RESP. You had some questions with respect to whether some points in the German eID make sense or not? 00:00:00

INT. Ah, yeah, can I just clarify something with you? If I understand correctly there's no data controller in the German eID scheme, correct? As in there's no Identity Provider.

RESP. No. Well...

INT. For citizens, not for Service Providers. Cause I know there's an Identity Provider that authenticates Service Providers...

RESP. Um, the original scheme was built without Identity Providers in the middle so
from a technical perspective you need to have an access certificate to access the
data on the eID card because you need to have this access certificate which is
used in the [...] protocol to establish the cryptographic channel between the card
itself and the Service Provider which is very nice from a security point of view and
because the citizens can be sure what kind of Service Provider wants to access his
data... this is also... and he needs to provide... he's forced to provide his consent
by entering the eID PIN, which is also very very nice from a privacy point of view
but now comes the real ground. The real ground is that this scheme which is very
nice from a security and privacy point of view is very costly. Because every Service
Provider needs to acquire such an access certificate which is only valid for two days
and when the system started there were three providers which issued such access
certificates but by now there's only one provider left. And in this situation.. so, the
prices are not decreasing but are of course because it's by now a monopoly they are
even increasing. So you need to... only for this access certificate you need to pay,
yeah, roughly 3.000€ a year and on top of this you need to acquire an eID service
which is another 10.000€ depending on the provider... there are different providers
but usually, yeah, roughly between 5.000 and 10.000€, so it's very costly. And the
consequence is that rather few Service Providers adopted the German eDI to accept
⏱00:04:23 the service, to access the eID card because of the high costs so in last summer they
changed the law to introduce the concept of Identity Provider, [name in German],
Identification Provider would be the correct translation... and this Identification
Provider needs to demonstrate again in a costly certification programme that he in
the end complies with certain security and privacy regulation based on ISO20001
and so the... in this case the... since last summer such an identification provider
will be able to act as an intermediary. And what [name of company] the scheme
is somewhat special because we had, we had such an access certificate and it was
strictly forbidden to share the data - to give the data to third parties, and we
circumvented the situation with [name of company] because we read out the data
and gave it to the end user. And in this case this is why we invented these derived
credentials so we, in this case, effectively the end user is able to pass over the data
which has been retrieved from the card to another Service Provider which otherwise
would have been not allowed. But since last summer they changed the eID law.

INT. Ok, so that means that the eID system effectively works the same way as it did before... you're not moving towards a model like Austria where they have a central hub?

RESP. No, no.

INT. Ok. Uh, and would you say that the system in Germany adhere to privacy by design?

⏱00:07:16 RESP. Absolutely. This is... from a privacy perspective, I think, the German system..

if you only look at security and privacy this is exactly how you would design a system. But from a practical point of view, the downside of this approach is that it's a little bit over engineered? It was very hard to implement it but now roughly 8 year after the introduction everything is working fine.. but this was a long way and it's still very costly. So from an economical point of view, it's not yet a success story.

INT. Would you see the way it's working changing once it's integrated into the Interoperability Framework of eIDAS? In other words, are there compromises?

RESP. Not really, because the general.. the technical aspect of eID cards they don't change. You still.. even after eIDAS, you need to have such, from a technical perspective, an access certificate to access the card. And, so the original approach to solve this problem was to assume that every Service Provider in Europe would get such an access certificate. Due to the eIDAS regulation I think that Germany as a member state is obliged to provide this access free of cost therefore I assume that if a public sector Service Provider from interestingly... I think there are good reasons that they must, that Germany must provide this access certificate free of charge. Because they need to provide this authentication procedure in cross-border settings free of charge. But what happens, so it's not clear to me whether this interpretation of eIDAS regulation is correct and what happens with German Service Providers. Because this would be something... new that German Service Providers they are...

INT. Yeah, you mean it's a bit unfair on them to have to pay for...

RESP. Yes, yes. So it's, the situation that Germans are discriminated actually because in a cross-border setting non-German Service Providers would get this certificate and eID service free of charge and the German ones would need to pay for it.

INT. But, so the way I understand it is that the German system defines pseudonyms according to a pair of user and Service Provider, correct?

RESP. Yeah...

INT. So, I mean, in the notification Germany has given over to the Commission they are specifying that every Member State is going to be considered one big Service Provider so they are going to provide one pseudonym per member state. Doesn't that change or reduce the privacy of the system?

RESP. It's not, I think it's not clear whether there will be a single... well.. probably yes, so the eIDAS node will become... for example the eIDAS node in Spain will become one Service Provider and it's... the eID card will produce a pseudonym which is tied to Spain. And of course the privacy, if you only consider the privacy aspect somewhat decreases, in theory at least. But, on the other side what often happens and this is what they are doing in [company name], or the same happens in Austria, we take this identifier which is produced by the eID and use it to create ⏱00:11:56

the sector specific and application specific new identifier. So the same could be done...

INT. In eIDAS nodes.

RESP. Yes, but it's, I think it's almost a matter of culture. So in Italy and Spain, in Spain for example the date of birth is part of the X.509 certificates. And so they obviously do not really care privacy issues...

INT. Yeah, but doesn't that effectively mean that by participating in a framework with all these countries you have to settle for the least private common denominator? So, in other words, Germans will have to accept that they need to give out their date of birth because Spain doesn't care about date of birth?

RESP. This is probably too, this conclusion is too...

INT. Simplified?

⏱00:14:31 RESP. Yes, yes. Because and this of course standardisation and collaboration on a European scale requires that a different member states and cultures somehow move together. And from a technical point of view of course this means that some Member States need to move to a common standard. This is very clear and natural, and from a privacy and security point of view it's also the case that this overall level in the long-term will become more equal but this doesn't necessarily mean that security and privacy is not important anymore. Because there are different ways of interpretation what security and privacy really means. As an example the video age verification is in Germany for qualified certificates according to Art. 24 of the eIDAS regulation is in Germany very limited and because of security reasons and other member states allow this and the argumentation is that video identification provides a higher level of conclusiveness and better evidence and therefore they consider it even more secure. And it is a little bit depending on...

INT. Interpretation...

RESP. Yes, on the interpretation which is ruled by culture in the end.

INT. What I'm basically trying to figure out is, is selective disclosure and pseudonyms, are they integral to Privacy by Design and is eIDAS compensating for not supporting them?

⏱00:16:57 RESP. That's a very very interesting question. I think if you consider what Privacy by design in identity management means there are good reasons to exactly put the requirement for the application of sector specific pseudonyms and selective disclosure, it's actually a must. Because if you do not have selective disclosure you have a conflict of the principle of minimising data, Article 5, and so this is without pseudonyms and selective disclosure it's hard to argue why a system fulfils privacy by design. So, the conclusion would be that eIDAS is not in line with, because the Minimum Data it's... includes not only the identifier but also first and last name i think which are transmitted.

INT. Yes and date of birth ⏱00:18:52

RESP. Yes. So in this case there are valid arguments why this is not in line with the GDPR.

INT. Well, to be pedantic about it eIDAS does not say it is going to support privacy by design, it says the Interoperability Framework will facilitate privacy by design. But my question is, how does it facilitate the privacy by design supported by the systems if it doesn't allow for selective disclosure and pseudonyms?

RESP. Yes, absolutely. Fully right. But in this area it's hard to discuss it with the Member States. So it's a very political process and probably you should.. it would be interesting to see what [name] is answering to this because he's very much involved in this highly political process...

INT. We've talked before about supporting pseudonyms in eIDAS nodes in the way that [name of company] does it. Wouldn't be as possible to support selective disclosure in eIDAS nodes? ⏱00:20:04

RESP. Sure. I think, I don't know whether there's an explicit requirement yet but this is something which is at least supported by best practice considerations. And this is probably the pragmatic way out, that the eIDAS nodes are trustworthy and they are trusted to take care that the privacy regulation which are, when eIDAS started there were different regulations, but by now they are harmonised and if there's an eID scheme which is not yet privacy friendly the eIDAS nodes, yeah, should be oblige to take care that this doesn't hurt in the end.

INT. I was browsing earlier the SAML attribute profiles, from the STORK project, and it seems that they are able to request specific attributes instead of requesting the whole minimum dataset so technically it is already... it doesn't need a change in the way that SAML exchanges happen, correct?

RESP. Yes, it will be an extension. In fact, a couple of years ago in the FutureID project we proposed such a privacy extension for SAML, I can dig out the paper. It's important to understand that to ask for certain attributes it's not part of the standard SAML protocol. You need to define an extension but this would certainly be possible. ⏱00:22:35

INT. Is that a paper you released in 2013? Cause I think I've read it.

RESP. Could be, I think so, I'll need to look it up but sounds possible.

INT. Ok. Well, if you have time later on I'll be really interested in reading it. One final thing, so up until now in most interviews I've done they seem to distinguish between the privacy that we should afford to public vs private services. So the general premise is that most public service will by de facto require most of the minimum dataset because that's the way public sector works but when it comes to private services, which shouldn't in principle require identification every time but they should do with authentication or less attributes....

00:23:42 RESP. Yes, I know this argument but it's not really valid. Because even in the... Austria shows that this is not necessary. You can establish a system where you only have identifiers between the different applications and if there is a need to provide the name and additional attributes this can be user-centric. So it's a little bit like... in Germany they issued a cyber security law which requires that every private company must inform the BSI [Federal Office for Information Security] if there's a security breach. And in the initial version was a paragraph that said this is only required for private organisation and public organisation do not need to notify any security breach. And just a few weeks before the law was passed there was an interesting security breach at the german parliament [Bundestag] so they changed this law to also include the public sector because this showed that security holes are also and probably especially in the public sector.

00:25:47 INT. So, you're saying that there is a way that public services can do with only minimal attributes not the whole minimum dataset?

RESP. Yes, it would certainly be possible.

INT. Brilliant. Um, right, I think I'm covered unless there's anything else you want to add?

RESP. Yeah I just looked at the document, I wasn't the author of this, but I just looked at it and [name] and colleagues were...

INT. Brilliant. Ok. Um, thank you very much. I'll probably gonna bother you again over the summer for data protection and the systems in FutureTrust.

RESP. What would be necessary to force the Member States to implement privacy by design? And it's, if I understood the fees related to the GDPR they are only applicable for private organisations as far as I see it so what could a EU citizen do to... would they need to sue the European Commission or all the member states possibly an interesting question.

INT. So the argument I'm working with at the moment is if it's not impossible and it's not out-of-this-world costly to allow Member States that have private system to use them as intended then the Commission should do that. So if that's in a form of an extra implementation directive, regulation or an extra standard that allows the eIDAS nodes to use the privacy design of the German system for example when the German system communicates with other member states then that should be allowed.

RESP. Yeah, ok.

INT. Yeah, so that's my working argument but we'll see how it goes...

RESP. Ok, perfect.

INT. Thanks very much.

RESP. Yeah, thank you.

B.5 Portugal

RESP. Hello? 00:00:00

INT. Good morning, [name]?

RESP. Hi, [name].

INT. Hi. Thanks for taking the time.

RESP. No problem. You're welcome.

INT. Let's get into it. So let me first explain what we are trying to get out of these interviews. So we are looking to understand how people that are working with eID think about Privacy by Design in modern eID systems and if what they think about, is present already in eIDAS or it can be accommodated for later. So can we just summarise how the Portugal system works. As far as I understand, there's the card and there's the mobile device that you can use for electronic identification?

RESP. Well, yes. There is a card that is a contact card. It has, well, two certificates, one for authentication and one for signature. And in addition to that, there's also a kind of data, the data file that contains the same information that is printed on the card, including the photo and that is freely… That can be read openly, as long as you introduce the card in a smartcard reader. And there's also another separate data file with the address and the address is protected by a PIN code.

INT. So the address is a protected attribute, but public attributes I'm guessing are names, date of birth? 00:02:11

RESP. Yes, the date of birth, the numbers, the ID numbers. So each ministry has one ID number. So social security, there is one ID. For the tax authority, there is another ID. And there's a civil registry ID which is, I'd say, the main citizen ID.

INT. So would you say these are sector-specific IDs?

RESP. Yes, sector-specific.

INT. But can different sectors read each other? So can the tax authority read the social security number for example?

RESP. Well, that depends. So what is read? So if you insert the card into a smartcard reader, you pull in all the information. So you read all the data file.

INT. But the reader is local to your machine, I'm guessing? 00:03:16

RESP. Yes, they use… Well, yes. There are some middleware that works via web interface.

INT. So in terms of transmitted attributes to the Service Provider, do all of these attributes get transmitted or it depends on what the Service Provider… Who the Service Provider is?

RESP. It's not visible, so it's not under the control of the user. When it is, let's say, read local, there is another way of authentication. That is through the Identity Provider, who is an Identity Provider for the public administration and exclusive just for Service Providers of the public administration. And there, you have control over the attributes that are transmitted. So it works like in STORK, if you're familiar?

INT. Yes.

RESP. When you go to the Identity Provider, you check that set of attributes that are requested. You can review them on the web page and then you authorise.

INT. How do you understand Privacy by Design in...? I don't know if you want to focus on the Portuguese system just or in general? It's up to you.

00:04:36 RESP. Well, I can just focus on the Portuguese eID, although I'm not official representative of ID schemes, so don't take this as an official answer from the government.

INT. This is why I said your opinion.

RESP. So in the Portuguese eID, they decided to separate these ID numbers for sector, say so [unclear]. And there is one ID per sector. And there is the Identity Provider that allows some review of the information. Well, there are the PIN codes, so there is one PIN for authentication, another one for the digital signature and another one for the address. And that's it basically. So there is not much control other than this.

INT. Would you say that way has any risks of linkability between uses or users?

RESP. Yes, there are some risks. For example, the authentication, the digital signature certificate, they have two or three fields that allows identification. So they have the subject's distinguished name with the full name of the person. There is one field that has the birth date of the user. And there is also another field that has the civil ID. And so whenever you use the card or certificate for authentication in a website, that can be collected from the website. Of course, there's also other fields like the subject key identifier. So I don't know if you're familiar with that field in a certificate, but it's basically a NASH over the public key. And so that's also, let's say, can be used for identification of the user. So it can be used that way.

00:06:59 INT. So that could play the role of a unique identifier in other words?

RESP. Yes, and the serial number of the certificates. So there are also all sorts of information that can be used for tracking the user. And let's basically think of certificates. Let's not avoid them.

INT. I think Belgium has the same issue or similar issues with [overtalking].

RESP. And probably Spain also because it's very similar. The systems are very similar. I know for example that in Norway, the ID number is... Well, there is only one ID number in the country, I guess, and it's not the presence in the certificates. What they do is for allow as Service Providers, they can retrieve the ID number from OCSP requests. So they get the certificate from the user and then they check the status against OCSP. And if it is an allow as Service Provider, the OCSP responds with the certificate status and also an extension with the ID number of the person.

INT. So that would be... The OCSP in that case would be some broker in between?

RESP. Yes, and of a resolver, something like that. 00:08:31

INT. So, so far what we have identified as main goals of Privacy by Design is data minimisation and unlinkability. And the way... What we've found so far in research is that the main techniques against linkability would be pseudonymisation and selective disclosure. Would you agree with that? Do you think there are other techniques that can be related?

RESP. Yes, there is one that is not... Well, it's known only on limit as, I'd say, a Cremic [unclear] forum, that is anonymous credentials.

INT. So like ABC for trusts?

RESP. Yes, exactly. And we are actually starting a project, an H2020 project that's called Olympus. So we are starting this project with IBM and IBMs from Switzerland, which is basically the investigator that started this anonymous credentials work. And local T [unclear], University of Murcia from Spain and, well, other partners, five or six partners. And so we are starting this project. Our particular aim for multisets is to integrate this technology into mobile driver's licence. And so explore the idea of not releasing, for example, the birth date if you are buying alcohol. Just answering if the person is over 18 or not.

INT. A yes or no answer.

RESP. So we're at... 00:10:25

INT. Would you say that these, well, all these technologies, so selective disclosure and pseudonymisation or a minimisation even. Can they be at present accommodated with eIDAS, the way eIDAS is being rolled out?

RESP. They can be at a close level. Well, data minimisation and selective disclosure, they can be through the STORK framework. So they can review information that you can share and all of that. So I believe that's working there. For the anonymous credentials, I think that can only work at a close... Within the scheme. So don't we interrupt roles because there are no standards in close [unclear] capability.

INT. So the way we view it, eIDAS asking for a minimum data set means that at least four attributes need to present at all times. Therefore we would like to make an argument that data minimisation can only be applied so far because you have to have at least these four attributes.

RESP. Well, I'm not that familiar. What attributes are that? Unless...

INT. It's a unique identifier which eIDAS says must be as persistent as possible in time and then first name, last name and date of birth. And then they have a set of optional attributes, which is address, place of birth and two others.

00:12:11 RESP. Yes, [unclear]. I think that is mostly oriented to public administration services because if you just want a presence online, I think of many services that will only think they need this email. They don't even need to know your name or ID. So I think that's mostly focused on public administration services.

INT. So would you say there's a case that seeing as the commission is trying to push eIDAS against private Service Providers as well, would you say there's a case to be made that, by public authorities and private authorities should be different, should be handled differently in terms of the data they receive? Would that be useful?

RESP. What I'm pretty sure is that private sector or, say, services, for sure don't need to know first name, last name. Most of the Internet services provider, there's SAS that's like that. They just need email or probably the phone number. Don't even need the email. So yes, by stating a minimum data set, we are actually narrowing the scope of services or expanding, actually expanding the data set. Because if a Service Provider needs just an email that the others are mandatory, you are actually increasing the data set not limiting. So maybe it makes sense for public administration services or government services to have a minimum data set. But for private sector it should be, well, defined if there's cases by basis.

00:14:25 INT. I'm guessing the same applies to the unique identifier as well?

RESP. Yes, exactly.

INT. So with that in mind, could pseudonymisation or selective disclosure... Well, you already said that selective disclosure can be applied through STORK. What about pseudonymisation? What about a scenario where the server of the sending state receives a unique identifier and then pseudonymises it to the receiving state, would that make sense?

RESP. My view on anonymous credentials is that, well, it is rather complex and there
are some performance impact at least from previous experience, so it doesn't really
work very well on smartcards or limited [unclear] devices . And my guess on this
is that they are just useful for offline scenarios because if you can reach a service,
then this can be answered trivially. So you are at the point of sale. If the point of
sale can contact a service, a public administration service that can respond whether
you are over or under 18, that is trivially answered. The difficulty is when you
are offline and you need to provide the adjustable answer to the point of sale. So
a sign of answer by the government but without, well, with information asked in
real time and provided with the confidence of the government, of the issuing of
that. So that, I think, is the challenge and there is where I see an opportunity
for... A need for anonymous credentials. Otherwise if you are online, that can be
implemented more easily. Also the offline solution as an additional benefit is that
00:16:51 it doesn't create a trail on the server. So for example if you are buying alcohol and
you need to contact a service online, you create a trail or a record, not only on the
vendor, but also on the state for example. And the state can see that you are, well,

asking too much questions about whether you are over 18 or not. So probably you are drinking too much alcohol or creating some profile or you are a smoker or with a work of gambling and stuff like that. So transactions that are offline are usually more privacy-friendly.

INT. So it would make it harder for services to profile you?

RESP. Exactly.

INT. So then wrapping up, would you say that eIDAS has room for improvement in terms of privacy?

RESP. Yes and in, it is for what I see now, it's mostly driven by the connections to the entry points. So they call it a connection void [unclear] box or stuff like that. So each country has its entry point, but it's mostly online. I believe providing infrastructure or the means for offline transactions would be also good for anonymous and for privacy.

INT. But wouldn't that… This is just for curiosity's sake. Wouldn't that require every country to have similar identification means? 00:18:24

RESP. Yes, interoperable, not… Well, what we'd require is a common definition on the formats of the information that is so on the credentials, that can be exchanged and a trust on the certification authority, so a trust list. So, for example, a vendor in Portugal accepting identification or anonymous credentials from a Spanish person and point of sales have to trust also on the CAs from Spain.

INT. But I guess that's already going to happen if Spain notifies eIDAS because the CA is not going to be the same?

RESP. Yes.

INT. Is there anything else that you would like to add? Because I'm covered, I think.

RESP. Let me just check here. You asked about how the ID scheme is operated in Portugal?

INT. Yes.

RESP. So it's managed by a public company. So it's a public entity for the government that outsourced a…

INT. Public cards. Service Provider 1 Public company, so the printing house in Portugal. And the printing house subcontracted parts of the service. So, for example, multiset is jointly operating the PKI with the prime contractor and also the public government. So I believe it's DPD on that. And about the notification, I don't believe we have yet… 00:20:11

INT. Announced.

RESP. Addressed the ID notification, the eIDAS notifications scheme. I think we are mostly relying on being on the TSL, on the trusted list and I think that's it.

INT. Thank you very much.

RESP. Welcome.

B.6 UK

00:00:00 RESP. The sent one was the one that [unclear] precedence and services request.

INT. Yes, that's because when the information sheet was resent the initial plan was to interview a lot more people. Then it became apparent that that is not going to be possible. Anyway, so shall I talk a bit about what I'm actually looking for before we start? So what I'm doing is I'm doing a PhD on electronic identities and I'm participating in an EU project called FutureTrust.

RESP. Okay.

INT. And what we are looking for is to see how Privacy by Design, if any, can be factored in eIDAS.

00:00:47 RESP. Can be, should have been, will be? It's an important distinction because the eIDAS is just a regulation so you're really talking about Privacy by Design either in the underlying eID system or in the interchange of data between systems enabled by eIDAS.

INT. Well, hopefully both because it's up to the national systems to decide what kind of Privacy by Design they want to have.

RESP. For the design of their systems.

INT. Yes, but then if they do decide on any kind then eIDAS should probably support it.

RESP. It would be stupid… If you built in something that is private an interchange mechanism cannot make it less private.

INT. Well yes, but that depends on how private it is in the first place.

RESP. Yes, but that's the design of the national system, not about the eIDAS interoperability [unclear].

INT. Yes, but for example if you look at the German system which is…

RESP. Chip on a smartcard, yes.

00:01:47 INT. Yes. We refer to it as the Ferrari of privacy at the moment. You don't have to agree with that, but in any case, it allows you selective disclosure, it allows you pseudonyms. Both of which things do not fully function in eIDAS.

RESP. At the level. So eIDAS in the sense of what data is shared with the foreign country?

INT. Yes.

RESP. That presumably is partly to do with what the relying party… So if you are a German in the UK and you wish to access government services, UK government services, then pseudonymisation is meaningless because that's not how the matching service works. So I don't think that's in the eIDAS issue. Let's say linking in to eIDAS system.

INT. Well, don't you think that eIDAS having a requirement to send a minimum data set by default means that by default you're going to receive a certain amount of identifiers, regardless of whether you need them or not?

RESP. Yes but given it's only three items it's pretty minimal and yes, you can argue that theoretically you are disclosing two items that you may not need for every task. But you also have the flipside that says: Oh, this is a service that's only requesting age or only requesting date of birth. Given that we know that there are 00:03:13 15 services online that can receive eIDAS codes, we've actually revealed that it's this one that's making the request, rather than sending the same data to everybody which is pretty minimal. And so it's not as clear cut as you might… As you are suggesting, that particularly in terms of which data you choose to share is actually more privacy preserving than sending the same fairly minimal, fairly contentious thing. Because you're talking about accessing government services…

INT. Initially.

RESP. Initially.

INT. Would that hold if in the future private Service Providers come into play?

RESP. Well, if they were only getting three data points then they're only getting three data points.

INT. Yes, but why should they have to get three data points?

RESP. Yes. No, I agree that you could build, but then what…? Yes, you could just say this is definitely a human to level… Whatever the… If you had a strong, significant or whatever it is. This is a human being and we know it's a human being registered in Germany, but that's all we're going to tell you. That's probably not an obvious 00:04:36 business model for most realistic services going forward. Yes, you can design ones that only need to know that you are a human being that a foreign government has recognised, but it's hardly… It's an interesting question and I'm working through my answer as I speak. But it's not a huge privacy risk and the number of services that would not want to, for example, personalise it by your first name is fairly limited realistically in a competitive marketplace at the moment with current privacy attitudes.

INT. Right, but should the attitude be towards what businesses want or what citizens want?

RESP. Okay, so explain to me how a citizen would want to access a private sector service that only confirms that somebody else has done some checking that they exist to a level of service credential.

INT. So for example… The example I have in my mind, and it's currently being tested in litigation, is Facebook. Say Facebook decides to use eIDAS for authentication. Technically…

RESP. Why would they want that?

00:05:57 INT. I don't know, but the Commission seems to think that they would. There was a communication last year inviting online social communities to. In any case, in a hypothetical scenario the only information Facebook really needs is that you're a human and you're above legal age. Now they have a policy now that they also request your real name, but this is what is being tested in Germany at the moment. So if you take Twitter for example who doesn't have the real policy name, all they need to know is that you're a human and you're a certain age. Why would I as a citizen want to disclose any more data than this and why should I have to?

RESP. No, I get the argument. So you want to have a way and are you therefore allowing…? Is Twitter therefore allowing the same human being to have multiple accounts? Which has to follow because you have no way of differentiating between two authenticated accounts from a foreign country.

INT. Yes. In theory you can have as many accounts as you wish. Which is replicated as well in some eID systems, right? So the UK system suggests that you can have multiple accounts for multiple Identity Providers.

RESP. Yes, you can. I've got ones with all of them.

INT. Good. You're the first person I meet who does.

00:07:32 RESP. I'm sure some of the GOV.UK people have as well.

INT. Probably. They're surprisingly hard to get a hold of. So then…

RESP. We'd better start recording because otherwise we're going to miss out some of the stuff.

INT. Yes, thank you. There we go. Yes. Right, can we start talking a bit about the Verify system?

RESP. Yes.

INT. So would you mind telling me how Verify…? What I know so far is it's a hub [unclear] system; there's a central hub. How does unlinkability…? Is unlinkability factored in the system?

RESP. Unlinkability defined how, sorry?

INT. Well, it depends on how you want to define it.

RESP. But I don't understand your question, so I can't answer your question until I know what you mean.

INT. Yes. So I believe that the basic premise is that the user and the Identity Provider are hidden from the Service Provider.

RESP. Yes, so that... So the hub... It's not completely unlinked because typically there're are some bits that are... So it's limited visibility rather than complete unlinkability, just from the way these things end up getting built. You connect to HMRC to do your self-assessment. It pings you to... You say you're going to use Verify, it goes to Verify. Verify asks you to log in with a pre-existing account or to create one if necessary when you've got a pre-existing one. You then authenticate with your IdP. Your IdP says... Does some background checks to make sure you're still not on that dodgy list of we gave you an account, but it's no longer valid and then sends a signed assertion to the hub confirming the matching data sets from the verified ID. And the hub then sends that back to the relying party, but the IdP only knows that you went to the hub and therefore to a government service at the moment and the relying party just knows the accounts from one of the certified companies. So there's no... So Experian as an IdP cannot know that you keep going to Universal Credit. It just knows you're going to government services. So you could be logging on 15 times to your Universal Credit, but you could also be tax returns, education, driving license. So they have no ability to get extra information about the transactions because they just know it's going to a government service. ⏱00:08:35

INT. Can two government services know that you're the same user? ⏱00:10:14

RESP. It depends how you define that because in practice each government service will typically have in its own records attached record for [name] and an education record for [name]. And so one level the answer is no because each IdP and relying party pair gets its own semi-persistent identifier. It can be refreshed. It's built that... So it's not persistent ID, it's a... Until someone asks or until we have a decision to have them timeout because there is obviously still a re-matching process that is involved. So sending to the hub [name] etc., going to HMRC and HMRC doing that matching is computational, less than for [name], but for other names. John Smith there would be quite a few, so you need to do a bit of extra work for the matching. So essentially they say: Until we get a... With a flag that says this hasn't changed there will also be a pairing flag that says it's the same [name] that logged on ten minutes ago because it's the same... Coming from the same IdP as etc. But that pairing is done IdP to relying party. So [name] using the same IdP to log onto two government services will have two of those unique semi-persistent identifiers.

INT. Sorry, just go back a bit. The pairing is happening IdP to relying party or hub to relying party? ⏱00:12:00

RESP. The hub does it, but essentially it's based on the IdP relying party pair.

INT. Okay because...

RESP. So [name] using Experian to log onto HMRC, there has to be some matching work out which tax record is [name]'s.

INT. Yes, understood, but as far as I understand…

RESP. Therefore you do that once if you log on with Experian, but equally I could have logged on with Barclays. And therefore you've got two paths and therefore you do not have the same persistent ID; you have two persistent IDs.

INT. And is the matching service keeping a record of the pairings? So I'm trying to figure out how reauthentication works. So if you visit that service a second time…

RESP. So the authentication is just done at the IdP. So the next time you log on you go to Barclays and Barclays says: Type in your username, password; we'll ping a code, one-time code, to your phone or whatever. And that's how the IdP knows that [name] is logged on again and then it says: Okay, it's definitely [name] or as far as we can tell it's definitely Edgar, and we're going to send his name, date of
00:13:27 birth etc., address history to the hub. And the hub then goes: Hey HMRC, you know you had this user with these things. Well, you've already worked out that it's tax record one, two, three, four, five so save yourself some time and go straight through to tax record one, two, three, four, five.

INT. But you said that the unique identifier might change from time to time?

RESP. Yes, so that's… So probably if I… So when you do your tax return every once in a while it times you out or asks you to confirm again. So it's semi-persistent. It's not a standard number that will remain for all time. It could be that if there is a real concern you just say every day it gets regenerated. So you're increasing the computational costs of the matching, but you are giving assurances that there's less persistence. It could be that when… If there's a break in service that you say regenerate everything. It could be that you had a panic about something, so you say regenerate things. So there's lots of ways. So it's a useful temporary number to allow for operational efficiencies and it therefore covers… And so one of the concerns people have had about eIDAS has been that wording of a persistent identifier. So it's persistent enough, but it's not persistent in their social security number type of persistent.

00:15:02 INT. So I'm guessing this can be to you… Can be thought of as one Privacy by Design…

RESP. Yes. Well, the whole thing is. The whole idea of a minimal matching data sets. The whole idea of storing the evidence that you use to confirm, to verify the ID in an offline, auditable on special request thing. The explicit design to have a single hub that separates that and limits the visibility. The idea of having multiple Identity Providers so that I could use Experian just to do my tax and Barclays just to do my health and… So if you know the system it makes no difference, but if you are slightly paranoid you can have different IdPs that only see different parts of your life. So Experian… So even if you didn't understand what the hub was doing, if you thought Experian could see you're logging into the tax authority, which is not the case, you can still say: I will use Experian for tax and Barclays for health, and Post Office for pensions. And therefore I am segmenting my life further.

INT. I'm guessing profiling from the services point is not an issue because they're public services.

RESP. Well, they've also got the data anyway. Why would they need to know that you're logged on from Experian if they just go along and say: We'll… Tax and, I don't know, rental income and income tax. It's all run by HMRC. You don't need to go to the bother… You really want to design the ID service and the hub so there's no interest in that. And if you want to know where Nicholas is logging in from then you go to Experian and say: Here's a warrant. If he logs in to do his tax return, please tell us from his mobile phone where you think he is and… Etc. 00:16:26

INT. Although in reality that would only show that I'm logging into the hub.

RESP. Right. Yes, but if you want… If we were trying to use the ID system to track you down there's no point in going to HMRC. So if we want to know where… What's happening with your money, we go to HMRC. If we wanted to know where you are logging in there's no point in going to HMRC, there's no point in going to the hub. Why not just go straight to the IdP? And that's a separate problem there, it's not a particular ID related problem.

INT. So in an imaginary scenario where Verify gets notified to eIDAS…

RESP. Yes. It's not necessarily imaginary, but yes.

INT. Yes, it just… As far as I know we haven't seen anything happening. So… 00:17:52

RESP. It's not… Nothing has yet happened. It's part of the whole EU negotiating trench of things. But obviously as a notifyee or recipient of notifications from September we've already got the Dutch I think. Somebody already notified.

INT. Germany has pre-notified and Italy I think.

RESP. Okay, and therefore everyone's doing the [unclear] level testing of what that actually means. So we'll definitely be receiving incoming because that's going live in September and that's… Well, assuming we can still be in Europe at that point, which is… It used to be the joke about well, we could always be kicked out before… We could be kicked out before GDPR comes in technically. I suspect we're not going to be kicked before either GDPR or the eIDAS notification bit happens, but technically, theoretically ministers still have to say: Assuming that we are blah blah blah. So we'll certainly be receiving those and we're responding to the pre-notifications etc. There's an awful lot of good sense to potentially notify before March 19 because nobody wrote the rules about what happens if you're outside of the EU, because it had not been anticipated at the time of eIDAS. So Brexit, the real Article 15, and it was there but nobody really worked through how we're going to do it. But there is nothing in eIDAS on the assumption that the Greeks will be 00:19:34

able to stay in the UK and Germans and French and Italians, and it's very unlikely that you will actually kick all Europeans out. Although again, between now and March never say never. But on the assumption that we're at least… Partly because we don't want all the pensioners back from Spain. On the assumption that it can be reasonably safe to assume that there will be Europeans in the UK it makes a lot more sense to have a single agreed process to allow them to potentially use their foreign created eIDs to access limited government services than not.

INT. So in a case where Verify gets notified how do you suggest it would work in eIDAS?

RESP. So receives a notification or…?

INT. No.

RESP. So the UK notifying Europe or Europe notifying…?

INT. UK notifying Europe.

RESP. Then in exactly the same way. Any Brits who are in the rest of Europe will be able to use their Verify ID as the official ID to access whatever services are available in those countries.

00:20:57 INT. I was wondering if there was an idea of would it be as a proxy or would it be as a middle… I can explain.

RESP. Okay.

INT. So eIDAS allows you to do two deploymentary systems. You can either deploy it as a proxy in your country where you operate the system and foreign services connect to your proxy who then sends back authentication data, the minimum data set. Or you deploy it as multiple instances locally in the foreign Service Provider.

RESP. I will be astonished if that happened.

INT. This is how Germany is doing theirs for example. So Germany's going to give every member state one instance of the system.

RESP. Okay, so Germany notifying to the UK. So UK hub linked services, tax records for example currently own… The government gave away the [unclear] and Verify. Those are the only two ways that you can get into…

INT. Well, so far, yes.

RESP. There's no time, no incentive, no plans that I'm aware of. We're certainly not going to let some German code access HMRC.

00:22:15 INT. Well…

RESP. It's not a…

INT. Yes, but isn't that the whole point of eIDAS being mandatory in that setting?

RESP. No, the whole point is we will receive the matching data set from Germany and Germany will say: This is definitely Hans to level substantial and this is the three data items that he will send, that we will send to the UK. And the UK goes: Right, we're quite happy. We have a process that actually sends a little bit more data, but here are the… Just the three data fields and we already have a matching data set service that the HMRC logs into. [Overtalking] and instead of taking a slightly larger verified data set it will take the slightly smaller German data set.

INT. So that's exactly what's going to happen. The only difference is that that data that Germany will send will come from UK territory because the server is going to be located in the UK and operated by the UK.

RESP. So they're going to duplicate all of their data?

INT. Well, technically they don't have to because all the data is in a citizen's card. So there's no Identity Provider to duplicate data.

RESP. So what's the German server in London doing then? 🕐00:23:30

INT. So the German… So a German citizen in the UK wants to go into HMRC. Goes to HMRC; HMRC asks them to log in. They have a card reader in their computer where they put their card in. Card reader reads the data, sends them… Sends it to Germany's eIDAS node located in the UK. The node says: Yes, that's legit. And sends back…

RESP. So I think the fact that there happens to be a node is an… I would see that as an implementation issue because that node could equally have been the Berlin node that sends exactly the same messages. So I don't see why that particular one is significant, other than that's how the Germans want to do it.

INT. So it seems significant to me because it changes the way their system operates. So their system in… Along the same lines as Verify to change the… So they're using a pseudonym as an identifier and it changes in every Service Provider. So…

RESP. But the matching data set…

INT. Is the same.

RESP. Has to be the same, doesn't it? It has to say Hans Schmidt, 1st August 1923.

INT. Yes. Well, that's in eIDAS. In Germany they don't have to disclose it. Yes.

RESP. But because… If the British tax system expects a name and a date of birth, giving him a random identifier is not going to help you get very far for the way the British systems are set up. 🕐00:24:58

INT. Agreed, but again that is an example of a system, of a service. There might be a service that needs less information, but that takes us back to the discussion we had before. What I wanted to point out is the way that they're deploying the system currently, it means that every… All services in a certain member state are going to be receiving the same pseudonym. So they're giving one pseudonym per user in every member state for public services and they've said that if private services come into play later on then the private services are going to have to apply for a different pseudonym in Germany.

RESP. Okay, that… But since the pseudonym bit is irrelevant for the UK because it's only the actual matching data set that they care about, it's irrelevant for the UK.

INT. So I think that's a point I want to make, that at the moment it's irrelevant for anything eIDAS because eIDAS expects the whole minimum data set. So my question, which might be a bit theoretical, is GDPR talks about pseudonymisation. Can you satisfy pseudonymisation without selective disclosure if you have to have a certain amount of data every time?

00:26:28 RESP. You wait for an activist to make a court case. It's not the top priority of any regulator anywhere for… Particularly where you've got all these other legitimate interested arguments for doing stuff.

INT. Okay. So you would say that the legitimate interest trumps the need for less data or justifies the need for this amount of data?

RESP. So we had the discussion a couple of days ago about if you have logged into HMRC, HMRC has sent you back to your own. You've done your various logins and they're now going to say: We're about to send this data so that you can access the government service. Do you need consent? For me to say yes is meaningless because you've already said that you want to do this. So you might want… So we have an interesting issue around the… You might know more of the technical detail. Your Greek records will be in the Greek alphabet. Your UK records might be transliterated, certainly spelt differently potentially, and equally so you… So we've got some Jannises with a J, some Ioannises with an I O A etc. and some others who say: Just call me John. And… So you've got a range of different ones, plus the actual alphabet thing, and if you do have existing records and it's even different spellings or even worse, different… I don't even know if it does UTC coding of the characters or just does Roman characters.

00:28:21 INT. Well, we have to. At least…

RESP. It's also a question of who's responsibility is it? Does the Greek system send out Roman characters?

INT. It's going to have to I believe, the same with passports. So we are required to have Latin characters in passports as well.

RESP. Okay, and do the German and Scandinavian umlauts and stuff…? Do those get…? It's…

INT. I don't know.

RESP. There is a simple… There is an answer, which is probably defined in the passport requirements, but… So that might address the character sets issue; it might not address the inaccurate multi versions of your: Is it Nick with a C K or Nik with a

K? Is it Nik or Nikos? That's... And potentially showing that this is the data that's going to come across. If you find that you can't log on an obvious one to check is whether they've actually got the spelling of this slightly non-standard name that we don't really recognise, that we may have misentered in our systems. That might be the first place to have a look to see.

INT. So in other words the argument you're making is that the amount of data we 00:29:33
currently have is a necessity when we absolutely need them?

RESP. The way the British systems have been designed is that it's based on that matching data sets because not having a unique identifier that you can use by sector, by service, by whatever... Or you've got multiple unique identifiers that are not completely population-wide or have horrible data like the UK National Insurance number. You just can't rely on that so you have to go back to the matching by name .

INT. Would you say there's a risk of...? So I get that we might not mind having our data in the services because they're public services and there's a certain amount of trust that we have. What about data in transit? So...

RESP. So through the Verify hub it's all encrypted. Now you can always improve that encryption. There also is a huge amount of active monitoring of, for example, device fingerprints . So what you were doing when the transaction started to the next stage etc.? To spot browser hijacking and stuff like that. Because these are all services that are basically giving out money and therefore they are a target for fraud. And it's a large country which is not poor, so there's an even larger... You may not choose to hack the Greek social security system, but you are going to hack... Try and break into the British one because there's money involved. So
from the very beginning security by design, as well as Privacy by Design, active 00:31:17
monitoring, all of those kinds of things. And equally pan governmental concerns that if part of the process has weaknesses that's going to affect everybody else because...

INT. So in that case would, and certainly in a cross-border scenario, would minimising the data be helpful to security?

RESP. Yes, and that's why it's a three item matching data set. And I suspect, and I don't know the technical detail, I would have thought... But just on the basis the Brits basically wrote it, that it will be encrypted then to end... So there's not very much and it's encrypted, and probably in practice if not in the regulations, there will be active monitoring of: Have things gone strangely wrong? Can we reset keys? Etc. So my sense is that that is kept under control and it's not one where I would be worrying too much.

INT. Right. So lastly, an idea that I'm still figuring out in my head, so I don't know. We were thinking what if... And this is in a scenario where we incorporate services that
do actually need less data than the minimum data set. Since you can't really in a 00:32:44

pragmatic sense find [unclear] to accept all Privacy by Design measures of every national system, what if selective disclosure was to be incorporated in the service? So for example Germany posts a server in the UK, sends over the minimum data set every time, but the server then selects which attributes to actually send to the end service.

RESP. Okay, so as I said this comes back to the earlier point that… Okay, we're still stuck talking about which of the three or something from those three, so a fair… You've not got much… Many scenarios of much flexibility.

INT. Well, in theory yes, it's because there're four optional ones as well.

RESP. Okay, but they're still a fairly constrained set and then you have the interesting question of how much information can you gain from the fact that the German server is only sending initials and a date of birth? Rather than everything. And this… It's the classic one of if you have secret monitoring bases and people know they probably exist, and all of a sudden you see an increase of traffic, communications traffic, you know that they're planning a war. So you spend… You make sure that the pipe is full of communications traffic the whole time, so that you don't spot a variation. A less well-planned one was the whole Fitbit and soldiers. So maybe we knew where the bases were, but if you suddenly see lots of soldiers running ⏱00:34:35 with their Fitbits you're going… Either they've all had a really big health kick or more likely there are more soldiers there and that is revealing information. So I think whilst the selective disclosure one is interesting and you could… The counter I think is the… By selectively disclosing you're actually revealing things that you did not want to reveal. So there was an interesting one of if you want a supportive verification process for people on Universal Credit and you want to pay the IdPs extra for helping people fill out the forms manually or having a call centre, then you've got to send a flag that says: Nikos is about to apply for Universal Credit and therefore please help him when he applies. So that's sending to the IdP [name] is receipt of Universal Credit and that's extra information that you may not have wanted…

INT. So in other words you're saying that the system might be able to infer that this particular user comes from Germany because he's…

RESP. Well, certainly if Germany is the only country that does that; one, they're German. Anything that is not the standard matching data set is German. Two, it's German and they're only sending initials and date of birth. It's a German applying for this service. At the time that there's only one service that… Where it's meaningful ⏱00:36:19 for that matching, for a subset of the matching data set to be sent. Now, then it becomes an interesting empirical question about proportionality; the relative benefits versus the potential disclosure. There's also a very practical level of you've got to run a load of code that's… So are you sending a…? It probably makes more sense to still send a matching data set, but with three of the fields being empty.

Or… And presumably…

INT. Or gibberish.

RESP. Yes, not meaning… Not the matching data for the matching data set. Do you have a flag says or do you assume that the relying party says: I know that this is a German one that only requires this, so I will not even look at the name field because I know it will be gibberish?

INT. Well, in theory you only need the relying party to say: This… These are the attributes I absolutely need. And then the…

RESP. But then you're changing, certainly in Verify, changing the hub model by saying: Give me… So there's… You either ask the hub to only send you certain fields or you receive all of the fields and only process the ones that you find helpful. So in the UK gender is a optional… It doesn't have to be disclosed. Some of the services don't use it for matching purposes. Some of them will use it if it's available. ⏱00:37:48

INT. So it's been a long time since I read the SA email exchange [unclear], but do services indicate which attributes they…?

RESP. No. They will just get name, date of birth, address and address history, and gender. And if it's not provided it's not provided.

INT. Okay. So they just send out a general request.

RESP. It's a…

INT. Give me everything you've got.

RESP. Well, it's give me what you give me. Which is everything in that matching data set and it's up to the relying party matching service to then choose which ones they actually look at.

INT. Ours too.

RESP. And part of that is the persistent ID and that if we already know that we've had… We've done that matching before and then we have the ability to connect it to the particular record.

INT. So in that case you don't need to do the whole process is what you're saying? ⏱00:38:53

RESP. Yes.

INT. Sorry, I've just… I've just been thinking, you mentioned proportionality as an empirical question.

RESP. So in that sense yes, there are some nice German-friendly theoretical benefits for not sending my surname when I request a particular service. Against… The flipside of that is if the horrible bad guys can spot a thing where it looks like… Let's say you can design it by just having a blank surname field. You can immediately spot any packets that have a blank surname field as being a German applying for that service and that is intelligence that lots of Germans are suddenly applying for this benefit say, which you may not… So it's… Are you better off not doing that and sending the data that gets ignored, versus not? So… And that's an empirical question and I think it's an academic empirical question given that we are talking about variations on a very small…

INT. Yes.

RESP. So a pragmatic one says the idea that your name and date of birth and…

INT. Address.

00:40:25 RESP. And address. Is that problematic? Less when you get to private ones. Does Facebook really need to know where I live potentially? And you might… But whether that would be done through eIDAS or whether that… There're other solutions to that one.

INT. It just… The argument I'm working against is that proportionality now has become a huge part of the GDPR. So the GDPR starts with the premise: Do the best you can or justify why you can't do it.

RESP. And the best you can says… I would feel quite happy going to whoever and saying: Doing it differently actually increases certain risks and a… Both increases certain risks and increases the complexity of the code. And increased complexity of code introduces additional risks as well. So this is not an unreasonable approach to take.

INT. That's a very interesting argument, thank you.

RESP. And particularly because we are talking about stuff… Particularly for private sector stuff where it's really academically… But the… Does Facebook need to know? So maybe not you're date of birth, but your age and so… And quite probably not your address. Is an interesting one, but then you go toward other things. Might it be reasonable that they know you've not been convicted of political corruption or
00:42:10 lying or… There's a whole load of other things that they…

INT. Well…

RESP. Or you move to an attribute exchange model that says: Actually, we're not doing an identity… Possibly come… The answer comes down to eIDAS is about identities, not attributes, and you can still have a verified identity too substantial that you then feed into an attribute exchange which is not covered by eIDAS. But if you've got every European country doing identity proofing too substantial and authentication too substantial, then linking that into an attribute exchange would be the way. I think that's the answer to your question. eIDAS is about identity and identity is identity, and attributes are a different thing. Still doesn't quite solve the Facebook doesn't need to know my address problem, but that's also commercial private sector reviews which is somewhere off…

INT. Well, that… There are differences in public sector reviews depending on the member state, but yes, I get what you mean.

RESP. I think if I was driving policy I would say what Facebook really wants is attributes. You're over 13 so we can't be prosecuted. And possibly some uniqueness, but that's a stupid business model choice for other than anything else. So I would say happy to reuse the verified substantial ID, but it's an attribute that you want and so
therefore it's not really… That's how I think… How I would push back on that if I 00:44:02
was asked by…

INT. Can you clarify something for me for Verify? Only because you're the first person I meet that has any connections with it.

RESP. Yes.

INT. As I understand at the moment Verify works in a level of assurance to…

RESP. Yes, they've also got LoA1 [unclear].

INT. So… Yes, so that would be… In eIDAS that would be low, correct?

RESP. Yes.

INT. So if they notify they're going to notify with that level of assurance presumably.

RESP. With two.

INT. With low?

RESP. With… Don't know. I… Do you notify? I don't know the details of what you're notified by. I would have thought you just say: We have an ID system that we wish to notify that you can consume tokens from. And one of the flags will be
substantial versus low. 00:44:58

INT. Yes. So eIDAS has the three levels. From substantial and upwards notification has mandatory effects to all other member states. In low you can notify the system, but then it's up to the other member states to accept it or not. So…

RESP. Okay, but realistically most useful… So an example of an LoA1 is viewing your driving license.

INT. Yes. So… Sorry, in what context?

RESP. So you can go to DVLA and you view the information on your driving license. That's LoA1, not LoA2. You cannot update your driving license on LoA1. So realistically most European government services of any use to any citizens are going to be LoA2.

INT. Yes. The question was mostly to make sure that…

RESP. So therefore I don't see any… So in terms of what you can do in the UK, most of the things… Because LoA2 came first and LoA1's only just been introduced, most
of the services already require LoA2 so… If Greece were to say: We're notifying 00:46:19
with LoA1 the UK might say get lost. It's not helpful. Or it might say: Fine. You can go and get the Greeks to view their British driving license, but they can't do anything else.

INT. Well, when you say LoA you mean the UK levels, right?

RESP. Yes. So Levels of Assurance. It's just different numbers.

INT. Because LoA1 cannot be notified. This is why I'm trying to figure out. I tried to double-check that LoA2 amounts to low in eIDAS.

RESP. No, substantial.

INT. Substantial?

RESP. Yes. I'm pretty sure. So we had LoAs and then Europe had something else, but
they are definitely cross-compatible because again the Brits basically wrote the
⏱00:47:09 rules or helped… Significantly helped write the rules. So LoA2 and substantial I
am pretty sure are the same thing.

INT. Brilliant. Right.

RESP. Don't quote me, but I'm pretty sure because it's… Because the one above substantial involved biometrics and [overtalking] whatever, and nobody's doing any of that. So it must be…

INT. Substantial.

RESP. Substantial rather than anything else.

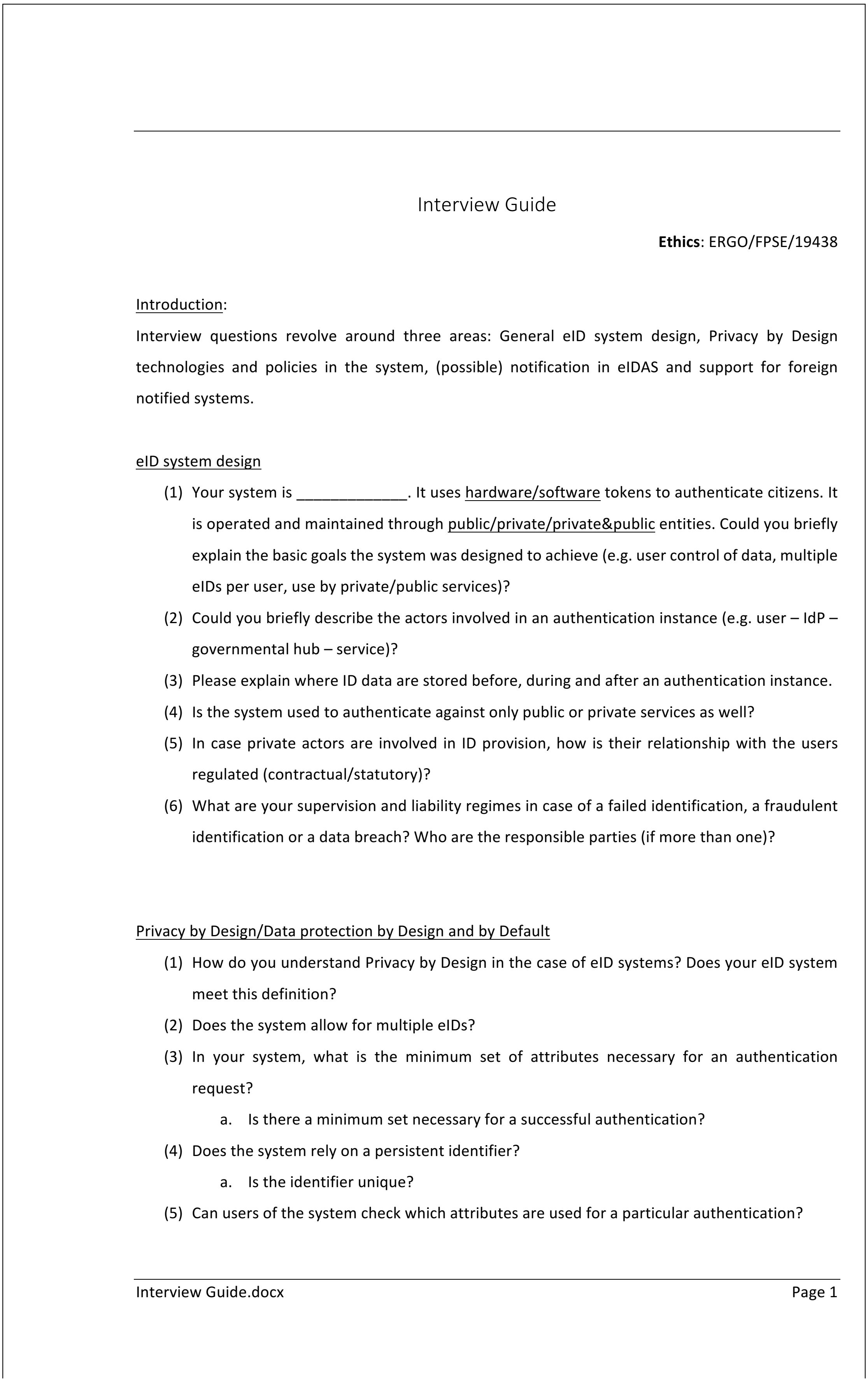
INT. Okay. Right. Well, I think I'm covered unless you have something else to add?

RESP. Nothing offhand.

INT. Let me just stop this. Saved it.

Appendix C

Interview guide for the semi-constructed interviews



Interview Guide

Ethics: ERGO/FPSE/19438

Introduction:

Interview questions revolve around three areas: General eID system design, Privacy by Design technologies and policies in the system, (possible) notification in eIDAS and support for foreign notified systems.

eID system design

(1) Your system is _____________. It uses hardware/software tokens to authenticate citizens. It is operated and maintained through public/private/private&public entities. Could you briefly explain the basic goals the system was designed to achieve (e.g. user control of data, multiple eIDs per user, use by private/public services)?

(2) Could you briefly describe the actors involved in an authentication instance (e.g. user – IdP – governmental hub – service)?

(3) Please explain where ID data are stored before, during and after an authentication instance.

(4) Is the system used to authenticate against only public or private services as well?

(5) In case private actors are involved in ID provision, how is their relationship with the users regulated (contractual/statutory)?

(6) What are your supervision and liability regimes in case of a failed identification, a fraudulent identification or a data breach? Who are the responsible parties (if more than one)?

Privacy by Design/Data protection by Design and by Default

(1) How do you understand Privacy by Design in the case of eID systems? Does your eID system meet this definition?

(2) Does the system allow for multiple eIDs?

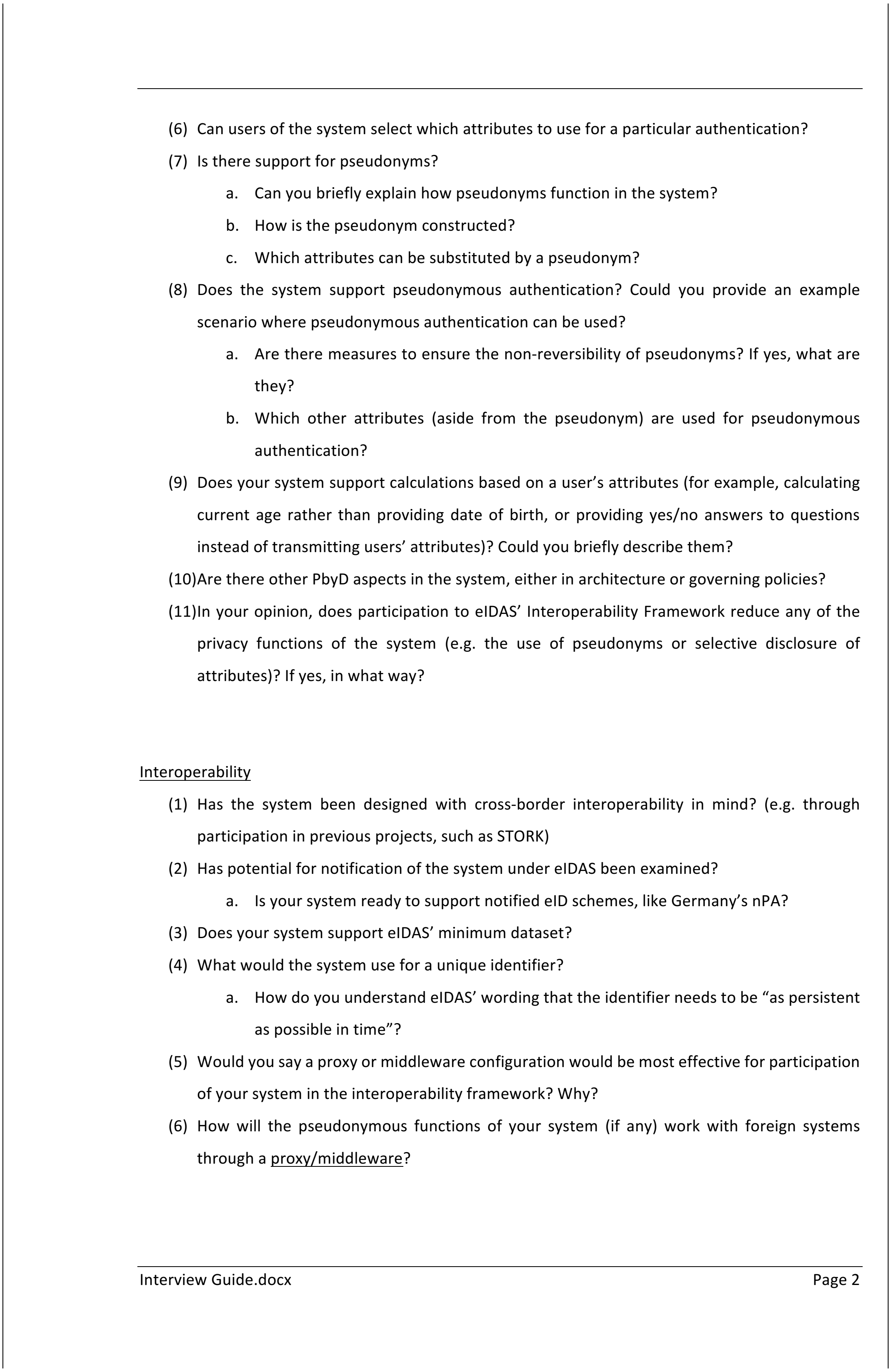
(3) In your system, what is the minimum set of attributes necessary for an authentication request?

a. Is there a minimum set necessary for a successful authentication?

(4) Does the system rely on a persistent identifier?

a. Is the identifier unique?

(5) Can users of the system check which attributes are used for a particular authentication?



(6) Can users of the system select which attributes to use for a particular authentication?

(7) Is there support for pseudonyms?

a. Can you briefly explain how pseudonyms function in the system?

b. How is the pseudonym constructed?

c. Which attributes can be substituted by a pseudonym?

(8) Does the system support pseudonymous authentication? Could you provide an example scenario where pseudonymous authentication can be used?

a. Are there measures to ensure the non-reversibility of pseudonyms? If yes, what are they?

b. Which other attributes (aside from the pseudonym) are used for pseudonymous authentication?

(9) Does your system support calculations based on a user's attributes (for example, calculating current age rather than providing date of birth, or providing yes/no answers to questions instead of transmitting users' attributes)? Could you briefly describe them?

(10)Are there other PbyD aspects in the system, either in architecture or governing policies?

(11)In your opinion, does participation to eIDAS' Interoperability Framework reduce any of the privacy functions of the system (e.g. the use of pseudonyms or selective disclosure of attributes)? If yes, in what way?

Interoperability

(1) Has the system been designed with cross-border interoperability in mind? (e.g. through participation in previous projects, such as STORK)

(2) Has potential for notification of the system under eIDAS been examined?

a. Is your system ready to support notified eID schemes, like Germany's nPA?

(3) Does your system support eIDAS' minimum dataset?

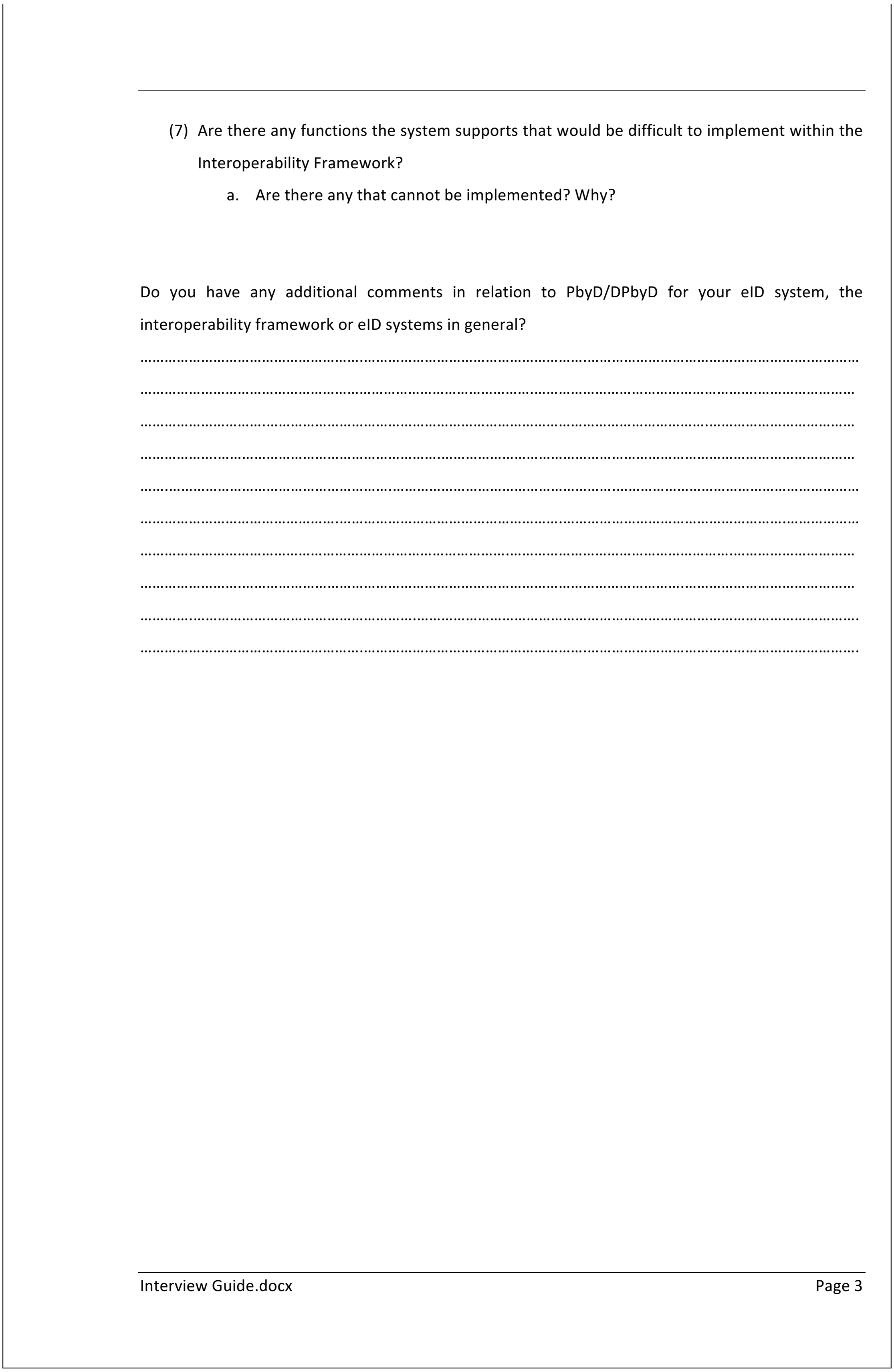
(4) What would the system use for a unique identifier?

a. How do you understand eIDAS' wording that the identifier needs to be "as persistent as possible in time"?

(5) Would you say a proxy or middleware configuration would be most effective for participation of your system in the interoperability framework? Why?

(6) How will the pseudonymous functions of your system (if any) work with foreign systems through a proxy/middleware?

Interview Guide.docx Page 2



(7) Are there any functions the system supports that would be difficult to implement within the Interoperability Framework?

   a. Are there any that cannot be implemented? Why?

Do you have any additional comments in relation to PbyD/DPbyD for your eID system, the interoperability framework or eID systems in general?

……

……

……

……

……

……

……

……

…….

…….

Bibliography

Bibliography

EU proposals

European Commission, *"Powers of the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority ***I Proposal for a directive of the European Parliament and of the Council amending Directives 98/26/EC, 2002/87/EC, 2003/6/EC, 2003/41/EC, 2003/71/EC, 2004/39/EC, 2004/109/EC, 2005/60/EC, 2006/48/EC, 2006/49/EC, and 2009/65/EC in respect of the powers of the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority"* COM(2009)0576 – C7-0251/2009 – 2009/0161(COD).

– *"Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Text with EEA relevance)"* COM (2012) 238 final.

– *"Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) No 575/2013 and (EU) 2019/876 as regards adjustments in response to the COVID-19 pandemic"* COM(2020) 310 final.

EU communications

EU Parliament: Committee on Employment and Social Affairs, *"Draft Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* (C7-0025/2012 – 2012/0011(COD), 8 November) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

European Commission, *"On Promoting Data Protection by Privacy Enhancing Technologies (PETs)"* (Communication) COM(2007) 228 final.

– *"A Digital Agenda for Europe"* (Communication) COM (2010) 245 final.

– *"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe"* (Communication) COM/2010/0245 f/2.

– *"Towards interoperability for European public services"* (Communication) COM(2010) 744 final.

– *"Towards interoperability for European public services"* (Communication) COM(2010) 744 final.

– *"A Digital Single Market Strategy for Europe"* (Communication) COM (2015) 192 final.

– *"EU eGovernment Action Plan 2016–2020"* (Communication) COM (2016) 179 final.

– *"Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe"* (Communication) COM(2016) 288 final.

– *"European Interoperability Framework – Implementation Strategy"* (Communication) COM (2017) 134 final.

Article 29 Working Party opinions

Article 29 Data Protection Working Party, *The Future of Privacy* (WP 168, 2009).

– *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 2010).

– *Opinion 3/2010 on the principle of accountability* (WP 173, 2010).

– *Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (WP 184, 2011).

– *Opinion 15/2011 on the definiton of consent* (WP 187, 2011).

– *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (WP 180, 2011).

– *Opinion 05/2012 on Cloud Computing* (WP 196, 2012).

– *Opinion 03/2013 on purpose limitation* (WP 203, 2013).

– *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (WP 223, 2014).

– *"Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)"* WP 240.

– *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev 01, 2017).

– *Guidelines on transparency under Regulation 2016/679* (WP 260, 2017).

EDPB, *"Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities"* Opinion 5/2019.

International standards

International Organization for Standardization, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model* (ISO/IEC 15408-1, 2009).

International Organization for Standardization, *Information technology – Security techniques – Privacy framework* (ISO:29100:2011, 2011).

International Organization for Standardization, *Information technology – Security techniques – Code of practice for information security controls* (ISO/IEC 27002:2013, 2013).

International Organization for Standardization, *Information technology – Security techniques – Guidelines for privacy impact assessment* (ISO/IEC 29134:2017, 2017).

Policy documents

Cabinet Office, *Framework Agreement and Schedules* (Draft v0,9, 2014) ⟨http://data.gov.uk/data/contracts-finder-archive/contract/1690273/⟩ accessed 24 August 2019.

Federal Office for Information Security [BSI], *"eIDAS Notification of the German eID"* (*Federal Office for Information Security*, 20 February 2017) ⟨https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html⟩ accessed 27 February 2017.

Privacy and Consumer Advisory Group, *Identity Assurance Principles* (v3.1, 2014) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1___4_.pdf⟩ accessed 26 May 2016 (archived at ⟨https://perma.cc/5K2W-8BVK⟩).

Technical reports

Agency for Public Management and e-Government, *Peer Review Report – United Kingdom's eID Scheme* (eIDAS Coordination Network, DG Connect, v 1.0, 2018) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/68326890/Final%20version%20of%20UK%20Peer%20Review%20Report_24_01_2019.pdf?version=1&modificationDate=1549037555551&api=v2⟩ accessed 28 July 2019 (archived at ⟨http://archive.fo/afbKM⟩).

Cabinet Office, *Identity Assurance Hub Service SAML 2.0 Profile v1.2a* (2013) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458610/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf⟩ accessed 23 July 2015 (archived at ⟨https://tinyurl.com/ybqjmo9h⟩).

Cantor S and others, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0* (OASIS Standard, 15 March, 2005) ⟨http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf⟩ accessed 27 February 2017.

eIDAS Technical Sub-group, *eIDAS – Interoperability Architecture* (v1.00, 2015) ⟨https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/82797006/eidas_interoperability_architecture_v1.00.pdf⟩ accessed 22 June 2019 (archived at ⟨https://tinyurl.com/vmao3rp⟩).

– *eIDAS SAML Attribute Profile* (v. 1.1.2, 2016) ⟨https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf⟩ accessed 4 November 2016 (archived at ⟨http://archive.fo/pLWy5⟩).

– *eIDAS SAML Message Format* (v 1.1.2, 2016) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_message_format_v1.0.pdf?version=1&modificationDate=1497252920416&api=v2⟩ accessed 4 November 2019 (archived at ⟨https://tinyurl.com/y6u2qnds⟩).

European Commission, *eIDAS-Node National IdP and SP Integration Guide* (v1.4.1, 2018) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/82772096/eIDAS-Node%20National%20IdP%20and%20SP%20Integration%20Guide%20v1.4.1.pdf?version=2&modificationDate=1554820110372&api=v2⟩ accessed 20 June 2018 (archived at ⟨https://tinyurl.com/yx5ta8px⟩).

Federal Office for Information Security [BSI], *Architecture electronic Identity Card and electronic Resident Permit* (Technical Guideline, TR-03127 v1.13, 2011) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf⟩ accessed 23 May 2016 (archived at ⟨http://archive.fo/IoGbj⟩).

– *“TR-03110 eIDAS Token Specification”* (*Federal Office for Information Security*, 5 January 2016) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?___blob=publicationFile~%5C&~v=1⟩ accessed 12 January 2016.

– *German eID based on Extended Access Control v2: Overview of the German eID system* (v1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_01_Whitepaper_final.pdf?version=1&modificationDate=1499172188962&api=v2⟩ accessed 22 February 2017 (archived at ⟨http://archive.fo/9Io5h⟩).

– *German eID based on Extended Access Control v2: LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance* (v1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_02_LoA%20Mapping_final.pdf?version=1&modificationDate=1499172189454&api=v2⟩ accessed 21 February 2017 (archived at ⟨http://archive.fo/qeJZE⟩).

– *German eID based on Extended Access Control v2: Fulfilment of interoperability requirements according to (EU) 2015/1501* (v1.2, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_03_IF%20Mapping_final.pdf?version=1&modificationDate=1499172189873&api=v2⟩ accessed 21 February 2019 (archived at ⟨http://archive.fo/GWzLJ⟩).

– *German eID based on Extended Access Control v2: Supporting Documentation* (v 1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_04_SuppDoc_final.pdf?version=1&modificationDate=1499172190074&api=v2⟩ (archived at ⟨http://archive.fo/IxFQ3⟩).

Government Digital Service, *Good Practice Guide (GPG) 45: Identity proofing and verification of an individual* (v. 4.1.1, 2019) ⟨https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual⟩ accessed 9 September 2019 (archived at ⟨http://archive.fo/a3bLF⟩).

Krevel F van, *PEER REVIEW REPORT – German eID* (DG Connect, Digital Single Market, eIDAS Cooperation Network, v 1.0, 2017) ⟨https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/Peer%20review%20report%20German%20eID%20-%2016062017.pdf?version=1&modificationDate=1499172190851&api=v2⟩ accessed 23 July 2019 (archived at ⟨http://archive.fo/3I24w⟩).

Secondary sources

32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (2010) ⟨https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf⟩ accessed 15 June 2019 (archived at ⟨http://archive.fo/fmxxB⟩).

Adler K, *"Brexit: UK and EU agree delay to 31 October"* *BBC News* (London, 11 April 2019) ⟨https://www.bbc.com/news/uk-politics-47889404⟩ accessed 20 May 2019 (archived at ⟨http://archive.fo/3DALG⟩).

AEPD, *List of the types of data processing that require a data protection impact assessment under Art. 35.4* (2019) ⟨https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2ZCHtjA⟩).

Aichholzer G and Strauß S, *"The Austrian case: multi-card concept and the relationship between citizen ID and social security cards"* (2010) 3(1) Identity in the Information Society 65 DOI: 10.1007/s12394-010-0048-9.

Alpár G and Hoepman J.-H, *"A Secure Channel for Attribute-based Credentials: [Short Paper]"* (Berlin, Germany, ACM Workshop on Digital Identity Management, 8 November 2013, DIM '13, ACM 2013) DOI: 10.1145/2517881.2517884.

Andrade MBG de and others, *Electronic Identity in Europe: Legal challenges and future perspectives (e-ID 2020)* (EUR 25834, 2013) DOI: 10.2791/78739.

Andrade NNG de, *"Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID"* (2012) 28(2) Computer Law & Security Review 153 DOI: 10.1016/j.clsr.2012.01.012.

Arapinis M and others, *"Analysing Unlinkability and Anonymity Using the Applied Pi Calculus"* (2010 23rd IEEE Computer Security Foundations Symposium, 17–19 July 2010) DOI: 10.1109/CSF.2010.15.

Argyrou A, *"Making the Case for Case Studies in Empirical Legal Research"* (2017) 13(3) Utrecht Law Review 95 DOI: 10.18352/ulr.409.

Arkel J van, Lange M, and Ryan H, *Towards an electronic ID for the European Citizen, a strategic vision: CEN/ISSS Workshop eAuthentication* (0.17, 2004) ⟨https://danishbiometrics.files.wordpress.com/2009/08/doc.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/rrykxr8⟩).

Banakar R, *"On the Paradox of Contextualisation"* in *Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity* (Springer International Publishing 2015) DOI: 10.1007/978-3-319-09650-6_5.

Barak A, *"Purposive interpretation in law"* (Princeton University Press 2007).

Barbaro M and Jr TZ, *"A Face Is Exposed for AOL Searcher No. 4417749" The New York Times* (New York, 6 August 2006) ⟨https://www.nytimes.com/2006/08/09/technology/09aol.html⟩ accessed 5 January 2020 (archived at ⟨http://archive.ph/QeAuG⟩).

Barnard-Wills D and Papakonstantinou V, *Best Practices for cooperation between EU DPAs* (Phaedra II project Deliverable 2.2, version 1.0, 2016) ⟨http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II_D2.2-report_2016.02.15.pdf⟩ accessed 15 March 2020 (archived at ⟨https://bit.ly/2LYtlZY⟩).

Barnard C, *Competence Review: The Internal Market* (Department for Business, Innovation and Skills, 2013) ⟨https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/226863/bis-13-1064-competence-review-internal-market.pdf⟩ accessed 20 November 2016 (archived at ⟨https://perma.cc/5NV2-EYJ2⟩).

Belgian Commission for the Protection of Privacy, *Recommandation relative au Registre des activités de traitements (article 30 du RGPD)* (Recommandation n^o 06/2017 (CO-AR-2017-011), 2017) ⟨https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/04/Belgian-Privacy-Commission-Recommendation_French.pdf⟩ accessed 25 April 2019 (archived at ⟨http://archive.fo/6a9nn⟩).

Bicknell D, *"Brexit brake on Verify spurs GDS to woo private sector on digital identity"* [2018] Government Computing ⟨https://www.governmentcomputing.com/brexit-eu/news/brexit-brake-verify-progress-spurs-gds-woo-private-sector-digital-identity⟩ accessed 30 April 2018 (archived at ⟨http://archive.fo/ZdTOj⟩).

Bieker F and others, *"A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation"* in Schiffner S and others, *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016) DOI: 10.1007/978-3-319-44760-5_2.

Bishop M, *"Introduction to Computer Security"* (Addison-Wesley Professional 2004).

Black D, *"Validating identity information against an authoritative source"* (*GovUK Verify Blog*, 10 October 2014) ⟨https://identityassurance.blog.gov.uk/2014/10/10/introducing-the-document-checking-service/⟩ accessed 2 August 2019 (archived at ⟨http://archive.fo/ZRvnM⟩).

Borking J, Verhaar P, and Blarkom GW van, *"PET"* in Borking J and others, *Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents* (PISA Consortium 2003) DOI: 10.13140/2.1.4888.7688.

Brandão L, Christin N, and Danezis G, *"Toward Mending Two Nation-Scale Brokered Identification Systems"* (2015) 2015(2) Proceedings on Privacy Enhancing Technologies 135 DOI: 10.1515/popets-2015-0022.

Brandom R, *"Making It Explicit. Reasoning, Representing, and Discursive Commitment"* (Harvard University Press 1994).

– *"Between saying and doing: Towards an analytic pragmatism"* (Oxford University Press 2008).

Brands S, *"Rethinking Public Key Infrastructures and Digital Certificates"* (The MIT Press 2000).

Burkert H, *"Privacy-enhancing Technologies: Typology, Critique, Vision"* in PE Agre and M Rotenberg (eds), *Technology and Privacy* (MIT Press 1997).

– *"Balancing informational power by informational power or Rereading Montesquieu in the internet age"*, in E Brousseau, M Marzouki, and C Méadel (eds), *Governance, Regulation and Powers on the Internet* (Cambridge University Press 2012) ⟨http://dx.doi.org/10.1017/CBO9781139004145.006⟩.

Burton C and others, *"The Final European Union General Data Protection Regulation"* (2016) 15 BNA Privacy & Security Law Report 153.

Bygrave LA, *"Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements"* (2017) 4(2) Oslo Law Review 105.

– *"Hardwiring Privacy"*, in Brownsword R, Scotford E, and Yeung K, *The Oxford Handbook of the Law and Regulation of Technology* (Brownsword R, Scotford E, and Yeung K eds, Oxford University Press 2017).

Cameron K, *"The Laws Of Identity"* (*Identity Blog*, 5 November 2005) ⟨http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf⟩ accessed 11 June 2015 (archived at ⟨http://archive.fo/LSkNo⟩).

Carey P, *"Data protection: a practical guide to UK and EU law"* (4th, Oxford University Press 2015).

Carolan E, *"The continuing problems with online consent under the EU's emerging data protection principles"* (2016) 32(3) Computer Law & Security Review 462 DOI: http://dx.doi.org/10.1016/j.clsr.2016.02.004.

Cavoukian A, *7 Laws of Identity the Case for Privacy-Embedded Laws of Identity in the Digital Age* (White Paper, 2006) ⟨http://www.ontla.on.ca/library/repository/mon/15000/267376.pdf⟩ accessed 11 June 2019 (archived at ⟨http://archive.fo/IaE5H⟩).

Cavoukian A and Dixon M, *Privacy and Security by Design: An Enterprise Architecture Approach* (2013) ⟨https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf⟩ accessed 20 January 2017 (archived at ⟨http://archive.fo/tVTPe⟩).

Centre for Information Policy Leadership, *Centre for Information Policy Leadership Comments on Data Protection Authorities' Draft List of Types of Data Processing Operations which Require or Do Not Require a Data Protection Impact Assessment* (2018) ⟨https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_national_dpa_lists_of_high_risk_processing.pdf⟩ accessed 8 May 2020 (archived at ⟨https://bit.ly/2SRB1B5⟩).

"Certificate Status Application" (*Secure Information Technology Center – Austria*, 2019) ⟨https://demo.a-sit.at/certificate-status-application/⟩ accessed 16 June 2019.

Chaum DL, *"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"* (1981) 24(2) Commun. ACM 84 DOI: 10.1145/358549.358563.

Chaum D, Fiat A, and Naor M, *"Untraceable Electronic Cash"* (Goldwasser S ed, Springer New York 1990) DOI: 10.1007/0-387-34799-2_25.

Chynoweth P, *"Legal research"* in A Knight and L Ruddock (eds), *Advanced research methods in the built environment* (Wiley-Blackwell 2008).

Clarke R, *"Privacy impact assessment: Its origins and development"* (2009) 25(2) Computer Law & Security Review 123 DOI: https://doi.org/10.1016/j.clsr.2009.02.002.

CNIL, *Privacy Impact Assessment (PIA): Measures for the Privacy Risk Treatment* (2015).

– *Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)* (2015) ⟨https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf⟩ accessed 15 August 2018 (archived at ⟨https://tinyurl.com/y9cqnmw4⟩).

– *Privacy Impact Assessment (PIA): Tools (templates and knowldge bases)* (2015) ⟨https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf⟩ accessed 15 August 2018.

– *Privacy Impact Assessment (PIA): Knowledge Bases* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf⟩ accessed 25 May 2019.

– *Privacy Impact Assessment (PIA): Methodology* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf⟩ accessed 25 May 2019.

– *Privacy Impact Assessment (PIA): Templates* (2018) ⟨https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf⟩ accessed 25 May 2019.

Conference of the Independent Data Protection Authorities of the Bund and the Länder, *The Standard Data Protection Model* (v1.0, 2017).

Cooper A and others, *Privacy Considerations for Internet Protocols* (RFC 6973, 2013) DOI: 10.17487/RFC6973.

Costa L, *"Data Protection Law, Processes and Freedoms"* in *Virtuality and Capabilities in a World of Ambient Intelligence: New Challenges to Privacy and Data Protection* (Springer International Publishing 2016) DOI: 10.1007/978-3-319-39198-4_6.

"Country overview" (*CEF Digital*, 2019) ⟨https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview⟩ accessed 12 September 2019 (archived at ⟨http://archive.fo/8tDw2⟩).

Craig P and Búrca C de, *"Instruments and the Hierarchy of Norms"* in Craig P and Búrca C de, *EU Law: Text, Cases, and Materials* (6th, Oxford University Press 1 July 2015).

Creswell JW and Plano Clark VL, *"Designing and Conducting Mixed Methods Research"* (3rd edition, SAGE 2017).

Crosby J, *Challenges and opportunities in identity assurance* (2008) ⟨http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf⟩ accessed 16 August 2015 (archived at ⟨https://perma.cc/D5RV-WM9U⟩).

Cuijpers C and Schroers J, *"eIDAS as guideline for the development of a pan European eID framework in FutureID"* (2014) 2014(237) Open Identity Summit 23.

Danezis G and others, *Privacy and Data Protection by Design – from policy to engineering* (ENISA report, 2014) DOI: 10.2824/38623.

Data Protection Inspectorate, *List of cross-border processing operations which are subject to the requirement for a data protection impact assessment* (2019) ⟨https://edpb.europa.eu/sites/edpb/files/decisions/ee_estonian_cross-border_dpia_list.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2zYrkdH⟩).

de Hert P and Papakonstantinou V, *"The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals"* (2012) 28(2) Computer Law & Security Review 130 DOI: http://dx.doi.org/10.1016/j.clsr.2012.01.011.

– *"Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?"* (2013) 9(2) A Journal of Law and Policy for the Information Society 271.

– *"The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit"* (2017) 33(3) Computer Law & Security Review 354 DOI: 10.1016/j.clsr.2017.03.008.

Deng M and others, *"A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements"* (2011) 16(1) Requirements Engineering 3 DOI: 10.1007/s00766-010-0115-7.

Directorate-General for Informatics (European Commission), *"New European Interoperabiliity Framework; Promoting seamless services and data flows for European public administrations"* (Publications Office of the European Union 30 November 2017) DOI: 10.2799/78681.

DLA Piper and others, *Proposal for a European IAS policy framework: Feasibility Study on an electronicidentification, authentication andsignature policy (IAS)* (Study carried out for the European Commission, D3, version 2b (final), 2013) ⟨https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2794⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ycg95yvm⟩).

Dumortier J and Vandezande N, *"Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market"* [2012] ICRI Research Paper 9 ⟨http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152583⟩ accessed 25 December 2016.

Duncan N and Hutchinson T, *"Defining and describing what we do: Doctrinal legal research"* (2012) 17(1) Deakin Law Review 83.

EFTA Court, *"The EEA and the EFTA Court: Decentred Integration"* (1st, Hart Publishing 2015).

eIDAS Observatory, *Principles and guidance on eID interoperability for online platforms* (final draft, 2018) ⟨https://ec.europa.eu/futurium/en/system/files/ged/draft_principles_eid_interoperability_and_guidance_for_online_platforms_final_draft_june_2018.pdf⟩ accessed 3 September 2019 (archived at ⟨http://archive.fo/Nx1Ua⟩).

El Emam K and Álvarez C, *"A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques"* (2015) 5(1) International Data Privacy Law 73 DOI: 10.1093/idpl/ipu033.

European Commission, *"Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200)"* (Commission Recommendation) C(2009) 3200.

European Commission, *"IMPACT ASSESSMENT: Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market "* (Commission staff working paper) SWD(2012) 135 final.

European Commission, *"On the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems"* (Commission Recommendation) 2014/724/EU.

European Commission, *Notice to Stakeholders: Withdrawal of the United Kingdom and EU Rules in the Field of Electronic Identification and Trust Services for Electronic Transactions* (2018) ⟨https://ec.europa.eu/info/sites/info/files/notice_to_stakeholders_brexit_e_signature_final.pdf⟩ accessed 14 April 2019 (archived at ⟨http://archive.fo/uYlcw⟩).

European Group on Ethics in Science and New Technologies, *Opinion on Ethics of Security and Surveillance Technologies* (No. 28, 2014) DOI: 10.2796/22379.

European Parliamentary Research Service, *eGovernment: Using technology to improve public services and democratic participation* (PE 565.890, 2015) ⟨http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA(2015)565890_EN.pdf⟩ accessed 25 May 2019 (archived at ⟨https://archive.fo/O4xX3⟩).

European Union Agency for Fundamental Rights, *"Handbook on European data protection law"* (2nd, Publications Office of the European Union 2014).

"Facebook's Name Policy" (*Facebook*, 2019) ⟨https://www.facebook.com/help/292517374180078⟩ accessed 10 September 2019 (archived at ⟨https://archive.fo/CEq7X⟩).

Falcón y Tella MJ, *"Case law in Roman, Anglosaxon and continental law"* (Martinus Nijhoff Publishers 2011).

Federal Office for Information Security [BSI], *IT-Grundschutz Methodology: BSI-Standard 100-2* (v 2.0, 2008) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile⟩ accessed 25 April 2019 (archived at ⟨http://archive.fo/nzytR⟩).

– *Technical Guideline TR-03130 eID-Server: Part 1: Functional Specification* (v 2.1.2, 2017) ⟨https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part1.pdf?__blob=publicationFile&v=3⟩ accessed 27 February 2019 (archived at ⟨http://archive.fo/5Njov⟩).

– *"The German eID"* (*Federal Office for Information Security*, 2017) ⟨https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html⟩ accessed 8 March 2017 (archived at ⟨http://archive.fo/gzHLy⟩).

Feiler L, Forgó N, and Weigl M, *"The EU General Data Protection Regulation (GDPR): A Commentary"* (Globe Law and Business 2018).

Gellert R, *"We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection"* (2016) 2(4) European Data Protection Law Review 481.

– *"On Risk, Balancing, and Data Protection: A Response to van der Sloot"* (2017) 3(2) European Data Protection Law Review 180 DOI: 10.21552/edpl/2017/2/7.

German L and others, *Consolidated report on the socio-economic basis for trust and trustworthiness* (D2.5, OPTET – OPerational Trustworthiness Enabling Technologies 2015) ⟨http://www.optet.eu/wp-content/uploads/deliverables/OPTET_WP2_D2.5_Consolidated_report_on_the_socio-economic_basis_for_trust_and_trustworthiness_v1.0.pdf⟩ accessed 10 October 2015 (archived at ⟨http://archive.fo/sqgts⟩).

Gibraltar Regulatory Authority, *(4) Data Protection Impact Assessments* (Guidance note, IR04/17 (v2), 2019) ⟨https://www.gra.gi/download/1020/GDPR4.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ydaukuqv⟩).

GovUK Verify, *"Privacy notice"* (27 June 2018) ⟨https://www.signin.service.gov.uk/privacy-notice⟩ accessed 23 May 2019.

Government Digital Service, *"Data from GOV.UK Verify"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/using-verify-data/data-from-verify/#data-from-gov-uk-verify⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/Jv8zF⟩).

– *"How SAML works with GOV.UK Verify"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/technology-overview/saml/#saml⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/wh1X6⟩).

– *"Technology Overview"* (*GovUK Verify Technical Guide*, 7 January 2018) ⟨https://www.docs.verify.service.gov.uk/technology-overview/#technology-overview⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/kmO8X⟩).

– *"Understand the different levels of assurance"* (*GovUK Verify Documentation*, 7 January 2018) ⟨https://www.verify.service.gov.uk/understand-levels-of-assurance/⟩ accessed 2 June 2019 (archived at ⟨http://archive.fo/k2w3o⟩).

Guest G, Bunce A, and Johnson L, *"How many interviews are enough? An experiment with data saturation and variability"* (2006) 18(1) Field Methods 59.

Hansen M, Jensen M, and Rost M, *"Protection Goals for Privacy Engineering"* (2015 IEEE Security and Privacy Workshops, San Jose, CA, May 2015) DOI: 10.1109/SPW.2015.13.

HDPA, *List of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of GDPR* (2018) ⟨http://www.dpa.gr/pls/portal/url/ITEM/7DBBF465EC436645E050A8C07C2422DA⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/3cYfOO9⟩).

Hildebrandt M and Tielemans L, *“Data protection by design and technology neutral law”* (2013) 29(5) Computer Law & Security Review 509 DOI: https://doi.org/10.1016/j.clsr.2013.07.004.

HM Government, *Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom* (2019) ⟨https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840656/Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2ZEFw6f⟩).

Hölbl M, *CEPIS – Position on the Electronic Identification and trust services (eIDAS)* (LSI SIN(15)01 v1.3, 2015) ⟨http://www.cepis.org/media/Position%20on%20the%20Electronic%20identification%20and%20trust%20services%20(eIDAS).pdf⟩ accessed 23 June 2019 (archived at ⟨https://tinyurl.com/yak94paz⟩).

Hornung G and Schnabel C, *“Data protection in Germany I: The population census decision and the right to informational self-determination”* (2009) 25(1) Computer Law & Security Review 84 DOI: 10.1016/j.clsr.2008.11.002.

Horsch M, Tuengerthal M, and Wich T, *“SAML Privacy-Enhancing Profile”* (Hühnlein D and Roßnagel H eds, Stuttgart, Germany, Gesellschaft für Informatik eV 2014).

Hufty M, *“Investigating Policy Processes: The Governance Analytical Framework (GAF)”* in U Wiesmann and H Hurni (eds), *Research for Sustainable Development: Foundations, Experiences, and Perspectives* (Geographica Bernensia 2011).

Hulsebosch B, Lenzini G, and Eertink H, *D2.3 – Quality authenticator scheme* (STORK deliverable, 3 March, 2009) ⟨https://joinup.ec.europa.eu/sites/default/files/document/2014-12/STORK%20Deliverable%20D2.3%20-%20Quality%20authenticator%20scheme.pdf⟩ accessed 29 July 2015 (archived at ⟨https://perma.cc/R5SH-DQG3⟩).

Hustinx P, *“EU Data Protection Law - Current State and Future Perspectives”* (Ethical Dimensions of Data Protection and Privacy, 9 September 2014, Centre for Ethics, University of Tartu / Data Protection Inspectorate, Tallinn, Estonia) ⟨https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf⟩ accessed 23 November 2016.

Hutchinson T, *“Researching and writing in law (3rd ed.)”* (Lawbook Co/Thomson Reuters 2010).

ICO, *Privacy Impact Assessment (PIA)* (2009) ⟨http://webarchive.nationalarchives.gov.uk/20091204132953/http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx⟩ accessed 20 September 2017.

ICO, *Conducting Privacy Impact Assessments: Code of Practice* (v 1.0, 2014).

ICO, *Preparing for the General Data Protection Regulation (GDPR)* (v2.0, 2017) ⟨https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf⟩ accessed 24 September 2019 (archived at ⟨http://archive.fo/8EuSp⟩).

ICO, *Data Protection Impact Assessments (DPIAs): The General Data Protection Regulation: Accountability and Governance* (v1.0.123, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf⟩ accessed 14 May 2019 (archived at ⟨http://archive.fo/dCyj4⟩).

ICO, *Guide to the General Data Protection Regulation* (1,0,154, 2018) ⟨https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf⟩ accessed 24 May 2018 (archived at ⟨https://tinyurl.com/y9pr9o2x⟩).

IDABC, *European Interoperability Framework for Pan-European eGovernment Services* (v1.0, 2004) ⟨https://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529⟩ accessed 6 January 2020.

Identity Assurance Team, *Identity Assurance Documentation: Release* (2015) ⟨http://docplayer.net/21642604-Identity-assurance-documentation.html⟩ accessed 24 August 2019 (archived at ⟨http://archive.fo/US2UC⟩).

Information Commissioner, ICO analysis of the Council of the European Union text of the General Data Protection Regulation (2016) ⟨https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf⟩ accessed 18 October 2016.

Ingram M, *"Why Twitter doesn't care what your real name is" GigaOM Technology Blog* (Austin, TX, 16 September 2011) ⟨https://gigaom.com/2011/09/16/why-twitter-doesnt-care-what-your-real-name-is/⟩ accessed 2 September 2019 (archived at ⟨http://archive.fo/ZZOiD⟩).

Jøsang A, *"Assurance Requirements for Mutual User and Service Provider Authentication"* (Garcia-Alfaro J and others eds, Springer International Publishing 2015).

Kemp R, Parto S, and Gibson RB, *"Governance for Sustainable Development: Moving from Theory to Practice"* (2005) 8(1/2) Int J Sustainable Development 12.

Khatchatourov A, Laurent M, and Levallois-Barth C, *"Privacy in Digital Identity Systems: Models, Assessment, and User Adoption"* in E Tambouris and others (eds), *14th International Conference on Electronic Government (EGOV), Aug 2015, Thessaloniki, Greece* (Lecture Notes in Computer Science, Springer International Publishing July 2015) vol LNCS-9248 DOI: 10.1007/978-3-319-22479-4_21.

Kloza D and others, *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals: d.pia.lab Policy Brief* (2017).

Knall T and others, *"Secure and Privacy-Preserving Cross-Border Authentication: The STORK Pilot 'SaferChat'"* (Andersen KN and others eds, Springer Berlin Heidelberg 2011).

Koops B.-J and Leenes R, *"Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law"* (2014) 28(2) International Review of Law, Computers & Technology 159 DOI: 10.1080/13600869.2013.801589.

Korff D, *Comparative Summary of National Laws: EC Study on Implementation of Data Protection Directive* (, Human Rights Centre, University of Essex 2002).

Koskenniemi M, *FRAGMENTATION OF INTERNATIONAL LAW: DIFFICULTIES ARISING FROM THE DIVERSIFICATION AND EXPANSION OF INTERNATIONAL LAW: Report of the Study Group of the International Law Commission* (International Law Commission, 58th session, General Assembly, A/CN.4/L.682, 2006).

Krzysztofek M, *"Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679"* (Wolters Kluwer 2017).

Le Métayer D, *"Privacy by Design: A Formal Framework for the Analysis of Architectural Choices"* (CODASPY '13, ACM 2013) DOI: 10.1145/2435349.2435361.

Leeuw F, *"Empirical Legal Research: The Gap between Facts and Values and Legal Academic Training"* (2015) 11(2) Utrecht Law Review 19 DOI: 10.18352/ulr.315.

Leitold H, *"Challenges of eID Interoperability: The STORK Project"* (Privacy and Identity Management for Life, 2011, Springer Berlin Heidelberg).

Letter from Andrea Jelinek on behalf of the European Data Protection Board to Sophie in't Veld MEP (5 July 2018) ⟨https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf⟩ accessed 3 January 2020 (archived at ⟨https://tinyurl.com/yxxawats⟩).

Levin O and Salido J, *The Two Dimensions of Data Privacy Measures* (Research Paper, Microsoft: Corporate, External and Legal Affairs 2016) ⟨https://fpf.org/wp-content/uploads/2016/11/The-Two-Dimensions-of-Data-Privacy-Measures.pdf⟩ accessed 28 November 2016 (archived at ⟨http://archive.fo/SfBCD⟩).

Malik T and Mittal A, *Technical Standards for Digital Identity Systems for Digital Identity* (World Bank Group's draft for discussion, 2017) ⟨http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf⟩ accessed 5 January 2020 (archived at ⟨https://tinyurl.com/ycegq9tm⟩).

Martens T, *"Electronic identity management in Estonia between market and state governance"* (2010) 3(1) Identity in the Information Society 213 DOI: 10.1007/s12394-010-0044-0.

Massacci F and Gadyatskaya O, *How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results* (White Paper, 2013) ⟨https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=whitepapers:seccord-eidas-whitepaper-2013.pdf⟩ accessed 27 January 2020 (archived at ⟨https://tinyurl.com/vn54l3n⟩).

Modinis IDM Study Team (ed), *Common Terminological Framework for Interoperable Electronic Identity Management* (techspace rep, 2.01, Europäische Gemeinschaft - eGovernment Unit 2005) ⟨https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf⟩ accessed 17 January 2020 (archived at ⟨https://tinyurl.com/yxyt942w⟩).

Neuman W, *"Social Research Methods: Qualitative and Quantitative Approaches"* (7th, Pearson, 2011).

OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview* (Committee Draft, 02, 2008) ⟨http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html⟩ accessed 19 January 2020 (archived at ⟨http://archive.is/V8Qb3⟩).

OASIS, *SAML V2.0 Subject Identifier Attributes Profile* (Committee Specification 01, Version 1.0, 2019) ⟨http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html⟩ accessed 17 February 2020 (archived at ⟨http://archive.is/ri9U6⟩).

Office of the Commissioner for Personal Data Protection, *Indicative List of Processing Operations Subject to DPIA Requirements under Article 35(4) of the GDPR* (2019) ⟨http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/ED786DE02E8020FCC225826000377143/$file/Indicative%20DPIA%20list.pdf⟩ accessed 20 May 2020 (archived at ⟨https://bit.ly/2WVoor9⟩).

OHara K, *"The Seven Veils of Privacy"* (2016) 20(2) IEEE Internet Computing 86 DOI: 10.1109/MIC.2016.34.

PBLQ, *International Comparison eID Means* (Final Report, 1.0, 2015) ⟨https://www.government.nl/binaries/government/documents/reports/2015/05/13/international-comparison-eid-means/international-comparison-eid-means.pdf⟩ accessed 2 June 2017.

Pfitzmann A and Hansen M, *Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology* (v0.33, 2010) ⟨https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.doc⟩ accessed 12 June 2015 (archived at ⟨https://tinyurl.com/ycshm2ey⟩).

Polish Data Protection Authority, *Proposed list of processing types for which a data protection impact assessment is mandatory* (2018) ⟨https://iapp.org/media/pdf/resource_center/Mandatory-DPIA-Poland-klattorneys.pdf⟩ accessed 22 June 2019 (archived at ⟨https://bit.ly/2Xpsjf6⟩).

Poller A and others, *“Electronic Identity Cards for User Authentication - Promise and Practice”* (2012) 10(1) IEEE Security & Privacy 46 DOI: 10.1109/msp.2011.148.

Probst T, *“Generische Schutzmaßnahmen für Datenschutz-Schutzziele”* (2012) 36 Datenschutz und Datensicherheit - DuD 439.

Rosner GL, *“Identity management policy and unlinkability: a comparative case study of the US and Germany”* (PhD thesis, University of Nottingham 2014).

Rössler T, *“Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government”* (2008) 24(5) Computer Law & Security Review 447 DOI: http://dx.doi.org/10.1016/j.clsr.2008.07.006.

Roßnagel H and others, *“FutureID – Shaping the Future of Electronic Identity”* (Limassol, Cyprus, Annual Privacy Forum 2012, 10–11 October 2012, 2012).

Rost M and Bock K, *Privacy by Design and the New Protection Goals* (EuroPriSe Whitepaper, 2011) ⟨https://www.european-privacy-seal.eu/AppFile/GetFile/ca6cdc46-d4dd-477d-9172-48ed5f54a99c⟩ accessed 9 February 2019 (archived at ⟨https://tinyurl.com/yazug8th⟩).

Rouvroy A and Poullet Y, *“The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy”* in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) DOI: 10.1007/978-1-4020-9498-9_2.

Sale JE, Lohfeld LH, and Brazil K, *“Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research”* (2002) 36(1) Quality and Quantity 43 DOI: 10.1023/A:1014301607592.

Schermer BW, Custers B, and Hof S van der, *“The crisis of consent: how stronger legal protection may lead to weaker consent in data protection”* (2014) 16(2) Ethics and Information Technology 171 DOI: 10.1007/s10676-014-9343-8.

Science and Technology Facilities Council, *UK e-Science Certification Authority Certificate Policy* (2.0, 2015).

Scott D, *“Resolving the quantitative–qualitative dilemma: a critical realist approach”* (2007) 30(1) International Journal of Research & Method in Education 3.

Shapiro S, *“What Is the Internal Point of View?”* (2006) 75(3) Fordham Law Review 1157.

Simma B and Pulkowski D, *“Of Planets and the Universe: Self-contained Regimes in International Law”* (2006) 17(3) The European Journal of International Law 483 DOI: 10.1093/ejil/chl015.

Slamanig D, Stranacher K, and Zwattendorfer B, *"User-centric Identity As a Service-architecture for eIDs with Selective Attribute Disclosure"* (SACMAT '14, ACM 2014) DOI: 10.1145/2613087.2613093.

Smart Grid Task Force, *Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment* (v. 2, 2018) ⟨https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf⟩ accessed 4 January 2020 (archived at ⟨https://tinyurl.com/ycj5l9vv⟩).

Smith A, Stirling A, and Berkhout F, *"The governance of sustainable socio-technical transitions"* (2005) 34(10) Research Policy 1491.

Somorovsky J and Mladenov V, *D2.2 Overview of eID Services* (FutureTrust Consortium, v 1.0, 2017).

Spiekermann S and Cranor LF, *"Engineering Privacy"* (2009) 35(1) IEEE Transactions on Software Engineering 67 DOI: 10.1109/TSE.2008.88.

Stalla-Bourdillon S and Knight A, *"Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data"* (2016) Forthcoming Wisconsin International Law Journal 1 ⟨http://eprints.soton.ac.uk/id/eprint/400388⟩ accessed 11 January 2017.

Stevens T, *Gov.UK Verify Data Protection Impact Assessment* (v 1.0, Government Digital Service, GovUK Verify blog 2016) ⟨https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf⟩ accessed 20 July 2019 (archived at ⟨http://archive.fo/p73oW⟩).

STORK, *Final Version of Technical Specifications for the cross-border interface: Secure idenTity acrOss boRders linKed 2.0 – STORK 2.0* (D4.11, 2015) ⟨https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174⟩ accessed 3 August 2018.

Strauß S and Aichholzer G, *"National Electronic Identity Management: The Challenge of a Citizen-centric Approach Beyond Technical Design"* (2010) 3(1) International Journal on Advances in Intelligent Systems 12.

Su J and others, *"De-Anonymizing Web Browsing Data with Social Networks"* [2017] Proceedings of the 26th International Conference on World Wide Web WWW '17 1261 DOI: 10.1145/3038912.3052714.

Suchman M and Mertz E, *"Toward a New Legal Empiricism: Empirical Legal Studies and New Legal Realism"* (2010) 6 Annual Review of Law and Social Science 555 DOI: 10.1146/annurev.lawsocsci.093008.131617.

Sullivan C, *"Digital identity, an emergent legal concept: the role and legal nature of digital identity in commercial transactions"* (University of Adelaide Press 2011).

Taekema S, *"Relative Autonomy, A Characterisation of the Discipline of Law"* in BJ van Klink (ed), *Law and Method. Interdisciplinary Research into Law* (Politika 4, Mohr Siebeck 2011).

"Terms of Service" (*Facebook*, 2019) ⟨https://www.facebook.com/legal/terms/plain_text_terms⟩ accessed 17 September 2019 (archived at ⟨http://archive.fo/mS3Rr⟩).

The Director General, *Annex to Reply from Information Society and Media Directorate General (INFSO) on CIS-Net* (Brussels, INFSO B1/RB Ares (2011), 2011).

Tsakalakis N, O'Hara K, and Stalla-Bourdillon S, *"Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation"* (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), 21 May 2016, Hannover, Germany, 2016) DOI: 10.1145/2908131.2908152.

Tsakalakis N and Stalla-Bourdillon S, *Deliverable 2.8: Documentation of the Legal Foundations of Trust and Trustworthiness* (Ref. Ares(2018)3469242 - 29/06/2018, FutureTrust consortium 2018) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/st7yes3⟩).

– *Deliverable 5.3: Legal evaluation of the FutureTrust architecture* (Ref. Ares(2019)4856595 - 25/07/2019, FutureTrust consortium 2019) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_6ee720db94a444b98f1cadafeefca1db.pdf⟩ accessed 5 September 2019 (archived at ⟨https://tinyurl.com/ycnogogd⟩).

Tsakalakis N, Stalla-Bourdillon S, and O'Hara K, *"What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation"* (Hühnlein D and others eds, Open Identity Summit, 15 September 2016, Rome, Italy, 2016) vol P-264 ⟨https://dl.gi.de/handle/20.500.12116/598⟩ accessed 12 January 2019.

– *"Identity Assurance in the UK: technical implementation and legal implications under eIDAS"* (2017) 3(3) The Journal of Web Science 32 DOI: 10.1561/106.00000010.

– *"Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?"*, in Kosta E and others, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers* (Kosta E and others eds, Springer International Publishing 2019) DOI: 10.1007/978-3-030-16744-8_17.

Tsakalakis N, Stalla-Bourdillon S, and Sel M, *Deliverable 2.7: State of the art in relation to privacy and data protection requirements: Preliminary report* (Ref. Ares(2017)522263 - 31/01/2017, FutureTrust consortium 2017) ⟨https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_ca38279654cc476fb24ecf5657b8be71.pdf⟩ accessed 25 May 2019 (archived at ⟨https://tinyurl.com/ujsvcwm⟩).

van der Sloot B, *"Editorial"* (2017) 3(1) European Data Protection Law Review 1 DOI: 10.21552/edpl/2017/1/3.

van Klink BJ and Taekema H, *"On the Border. Limits and Possibilities of Interdisciplinary Research"* (van Klink BJ and Taekema H eds, Mohr Siebeck 2011).

Vandezande N, *"Identification numbers as pseudonyms in the EU public sector"* (2011) 2(2) European Journal of Law and Technology, 1 ⟨http://ejlt.org/article/view/65/142⟩.

Veale M, Binns R, and Ausloos J, *"When data protection by design and data subject rights clash"* (2018) 8(2) International Data Privacy Law 105 DOI: 10.1093/idpl/ipy002.

Veeningen M, Weger B de, and Zannone N, *"Data minimisation in communication protocols: a formal analysis framework and application to identity management"* (2014) 13(6) International Journal of Information Security 529 DOI: 10.1007/s10207-014-0235-z.

Verhaeghe P and others, *"Security and Privacy Improvements for the Belgian eID Technology"* in Gritzalis D and Lopez J, *Emerging Challenges for Security, Privacy and Trust: 24th IFIP TC 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18–20, 2009. Proceedings* (Gritzalis D and Lopez J eds, Springer Berlin Heidelberg 2009) DOI: 10.1007/978-3-642-01244-0_21.

Warren AP and others, *"Privacy Impact Assessments: the UK experience"* (31st International Conference of Data Protection and Privacy Commissioners, 4–6 November 2009, Madrid).

Webley L, *"Qualitative Approaches to Empirical Legal Research"* in P Cane and HM Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2012).

White Wire Data Protection, *Data Protection Impact Assessment* (Template, 2017) ⟨https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6590736/bin/18-1421-Techapp-s3.pdf⟩ accessed 26 May 2018 (archived at ⟨https://tinyurl.com/ybc5fz9q⟩).

Whitley E and Hosein G, *"Global Challenges for Identity Policies"* (plagrave macmillan 2010) DOI: 10.1007/978-0-230-24537-2.

Wright D and others, *A Privacy Impact Assessment Framework for data protection and privacy rights: PIAF Project* (Deliverable D1, 2011).

Wright T and Hustinx P, *Privacy-Enhancing Technologies: The Path to Anonymity* (Volume 1, 184530, 1995) ⟨http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf⟩ accessed 23 May 2019 (archived at ⟨http://archive.fo/0p30U⟩).

Wuyts K and Joosen W, *LINDDUN privacy threat modeling: Privacy knowledge (tables)* (Technical Report (CW Reports), Department of Computer Science, KU Leuven 2015) ⟨https://linddun.org/downloads/LINDDUN_tables.pdf⟩ accessed 25 April 2018.

– *LINDDUN privacy threat modeling: a tutorial* (CW reports, CW685, Department of Computer Science, KU Leuven 2015) ⟨https://7e71aeba-b883-4889-aee9-a3064f8be401.filesusr.com/ugd/cc602e_f98d9a92e4804e6a9631104c02261e1f.pdf⟩ accessed 7 January 2020.

Yee GO, *"Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards"* (IGI Publishing 2011).

Yin RK, *"Case Study Research: Design and Methods"* (5th, SAGE Publications 2014).

Zuccherato R, *"Entity Authentication"* in HC van Tilborg and S Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US 2011).

Zwattendorfer B and Slamanig D, *"On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud"* in LJ Janczewski, HB Wolfe, and S Shenoi (eds), *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings* (Springer Berlin Heidelberg 2013) DOI: 10.1007/978-3-642-39218-4_23.

Zwingelberg H and Hansen M, *"Privacy Protection Goals and Their Implications for eID Systems"* (Camenisch J and others eds, Springer Berlin Heidelberg 2012) DOI: 10.1007/978-3-642-31668-5_19.

Zwingelberg H and Schallaböck J, *H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective* (v1.0, ABC4Trust 2013) ⟨https://abc4trust.eu/download/ABC4Trust-H2.4_Privacy_Perspective_on_the_eIDAS_regulation.pdf⟩ accessed 12 May 2016 (archived at ⟨http://archive.fo/1kPEw⟩).