OPerational **T**rustworthiness **E**nabling **T**echnologies

D2.5 – Consolidated report on the socio-economic basis for trust and trustworthiness

Stefanie Wiegand et al.

Document Number	D2.5
Document Title	Consolidated report on the socio-economic basis for trust and trustworthiness
Version	1.0
Status	Final
Work Package	WP 2
Deliverable Type	Report
Contractual Date of Delivery	31/10/15
Actual Date of Delivery	31/10/15
Responsible Unit	IT Innovation
Contributors	Laura German, Costas Kalogiros, Michalis Kanakakis, Bassem Nasser, Sophie Stalla-Bourdillon, Shenja van der Graaf, Wim Vanobberghen, Stefanie Wiegand
Keyword List	Trust, Trustworthiness, Semantic modelling, User trust
Dissemination level	PU

Document Review

Review	Date	Ver.	Reviewers	Comments
Outline	16/06/2015	0.1		
Draft	15/10/2015	0.2		added iLaws contribution
	20/10/2015	0.3		updated ToC and sorted contributers alphabetically
	20/10/2015	0.4		added AUEB contribution
	21/10/2015	0.5		sorted iLaws references
	23/10/2015	0.6		checked (cross-)references
	26/10/2015	0.7		added missing sections and did some more spell-checking
	28/10/2015	0.8		proof-reading, updated reference list, re-formatting
	30/10/2015	0.9		merged reviews
	30/10/2015	1.0		finalised document
QA			Torsten Bandyszak (UDE) Michel Varkevisser (TNL)	
PCC				

Glossary, acronyms & abbreviations

DPbyD	Data Protection by Design
DPA	the Data Protection Act 1998 (UK)
DPIA	Data Protection Impact Assessment
DTTM	Design Time Trustworthiness Model
DTwC [1]	Digital Trustworthiness Certification
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ICT	Information and Communication Technologies
IEC	International Electro-technical Commission
ISO	International Organization for Standardization
ITU	International Telecommunications Union
OPTET	Operational Trustworthiness Enabling Technologies
OPTET-LIM	OPTET Legal Integration Model
OWL	Web Ontology Language
PbyD	Privacy by Design
PIA	Privacy Impact Assessment
SLA	Service Level Agreement
SSD	Secure System Designer
STS	Socio-Technical System
TME	Trust Metrics Estimator
TWbyD	Trustworthiness by Design
WP	Work Package

Executive Summary

This deliverable provides a public consolidated report on the socio-economic basis for trust and trustworthiness in OPTET. It summarises the basic definitions of trust and trustworthiness that laid the foundation of developing trust and trusworthiness enabling technology over the different OPTET WPs.

Trust in a system is defined as a property of a stakeholder (known as the trustor) reflecting the strength of their belief that engaging in the system for some purpose will produce an acceptable outcome. Trustworthiness on the other side is a property of the system. A system is more trustworthy if it is able to produce an outcome acceptable to all trustors.

The approach taken by OPTET WP2 involves the use of several different models during the design and operation of the system. A conceptual unifying model is presented in this deliverable. At the heart of this model is a semantic model of system trustworthiness, in which threats to the system are described in relation to groups of interacting system assets.

The repeated findings throughout all the exploratory analyses showed that we can cluster users into segments of similar trust-related behaviour.

The foundation established by WP2 has been leveraged by the different OPTET WPs in order to incorporate and manage trust and trustowrthiness over the socio-technical system lifecycle. This includes design, development and certification, distribution and deployment as well as maintenance phase. A specific emphasis in this deliverable is put on the possible future legal measures that are likely to have a role in the overall approach to a trusted Future Internet. The two approaches – trustworthiness-by-design (TWbyD) and data-protection-by-design (DPbyD) – are critically assessed through cross-comparative evaluation. As a result of this critical analysis, this section identifies a need for greater legal integration across the ICT platform lifecycle in order to strengthen a value-by-design approach to a trusted Future Internet environment. In consequence, it proposes the OPTET Legal Integration Model (OPTET-LIM) aimed at raising legal awareness and interdisciplinary exchange from the ICT platform design stage. Finally, it briefly explores the newest legal instrument that explicitly aims at promoting trust online – the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) Regulation – including its connection to value-by-design and explains why a TWbyD approach is crucial in such an environment.

This deliverable discusses the need for an OPTET Legal Integration Model to support TWbyD in the scope of the OPTET lifecycle. The OPTET-LIM framework is aimed at raising legal awareness and interdisciplinary exchange from the ICT platform design stage, and will be reusable for other, trusted Future Internet applications.

We also give an overview of the OPTET models and the OPTET lifecycle on which the legal models are proposed to be applied.

Table of Contents

1. Introduction

This deliverable provides a public consolidated report on the socio-economic basis for trust and trustworthiness in OPTET.

Trust in a system is defined as a property of a stakeholder (known as the trustor) reflecting the strength of their belief that engaging in the system for some purpose will produce an acceptable outcome. Trustworthiness on the other side is a property of the system where the Oxford English definition (trustworthy = honest, truthful and capable, i.e. worthy of someone else's trust). A system is more trustworthy if it is able to produce an outcome acceptable to all trustors.

In practice, a system becomes less trustworthy if its behaviour suggests that it may be subject to active threats. An active threat is a situation or event that has arisen and is producing consequences for the system behaviour and outcomes. An active threat doesn't necessarily lead immediately to an unacceptable outcome, but it indicates that something is happening that threatens the system's ability to avoid such an outcome. This leads to the idea that one can quantify trustworthiness via the probability that potential threats are active, and hence that the eventual outcome will be unacceptable.

The approach taken by OPTET WP2 involves the use of several different models during the design and operation of the system. A conceptual unifying model is presented in this deliverable. At the heart of this model is a semantic model of system trustworthiness, in which threats to the system are described in relation to groups of interacting system assets. By using a semantic model, we automate much of the reasoning underlying the OPTET procedures, enabling complex analysis previously done by humans to be applied at composition and run-time. This ensures that system designers do not need so much expertise in how threats might apply to their system and that they cannot simply overlook or ignore threats thus making the results less subjective than a conventional risk-based approach.

Situations that may raise user concerns and so potentially affect their behaviour are therefore included as threats in the model. These threats can be used as a basis for defining what is meant by trust (i.e. a belief that the system will address the user's concerns by blocking or otherwise mitigating against these threats). This is a multi-dimensional approach to trust. The major objective of our trust computation research activity was to identify socio-technical and economic factors affecting the subjective nature of trust, and formulate them into theoretical models in a mathematical concrete way. The repeated findings throughout all the exploratory analyses showed that we can cluster users into segments of similar trust-related behaviour. The foundation established by WP2 has been leveraged by the different OPTET WPs in order to incorporate and manage trust and trustowrthiness over the socio-technical system lifecycle. This includes design, development and certification, distribution and deployment as well as maintenance phase.

A specific emphasis in this deliverable is put on the possible future legal measures that are likely to have a role in the overall approach to a trusted Future Internet. The two approaches – trustworthiness-by-design (TWbyD) and data-protection-by-design (DPbyD) – are critically assessed through cross-comparative evaluation. As a result of this critical analysis, this section identifies a need for greater legal integration across the ICT platform lifecycle in order to strengthen a value-by-design approach to a trusted Future Internet environment. In consequence, it proposes the OPTET Legal Integration Model (OPTET-LIM) aimed at raising legal awareness and interdisciplinary exchange from the ICT platform design stage. Finally, it briefly explores the newest legal instrument that explicitly aims at promoting trust online – the Electronic Identification and Trust Services for

Electronic Transactions in the Internal Market (eIDAS) Regulation – including its connection to value-by-design and explains why a TWbyD approach is crucial in such an environment.

This document is organised as follows. Section 2 will give an overview of the OPTET Trust and Trustworthiness Models. In section 3, we explain how these models fit into the OPTET Workflow and how they are applied within the different work packages. Section 4 then discusses the design of a legal framework required to support PbyD and TWbyD. Finally, section 5 outlines the key findings and indicates how they can be applied.

2. OPTET Trust and Trustworthiness Model

This section presents the conceptual unified model of trust and trustworthiness in OPTET. It also goes through the details of the trustworthiness and trust modelling highlighting the approach taken and the results.

2.1. Conceptual model

The purpose of the OPTET WP2 modelling is to address the following main challenges:

- System designers often lack security expertise to identify potential threats to their systems and the countermeasures. They may overlook threats they do not understand, or that they subjectively believe are not important for their particular system. The automation proposed in OPTET addresses this issue making the threat identification process more transparent and auditable
- ICT Risk-based methods are helpful in addressing system vulnerabilities at design time; however, they are not well related to socio-economic concepts of trust and trustworthiness.
- There is a separation between design-time and runtime risk analysis. Information from design-time risk-based analysis is not fully utilised systematically at run-time.

The last of these points is due partly to the fact that risk analysis still largely depends on humans with relevant expertise (even if assisted by a standardised procedure and check list). Run-time analysis is only useful if it can be done rapidly when systems change or their behaviour and status change. This often means risk-based analysis cannot be used at all when considering dynamically composed (e.g. Future Internet) systems. The approach taken by OPTET WP2 involves the use of several different models during the design and operation of the system. This separation of design-time and run-time activities to be performed based on the different models and artefacts is shown in Figure 1.

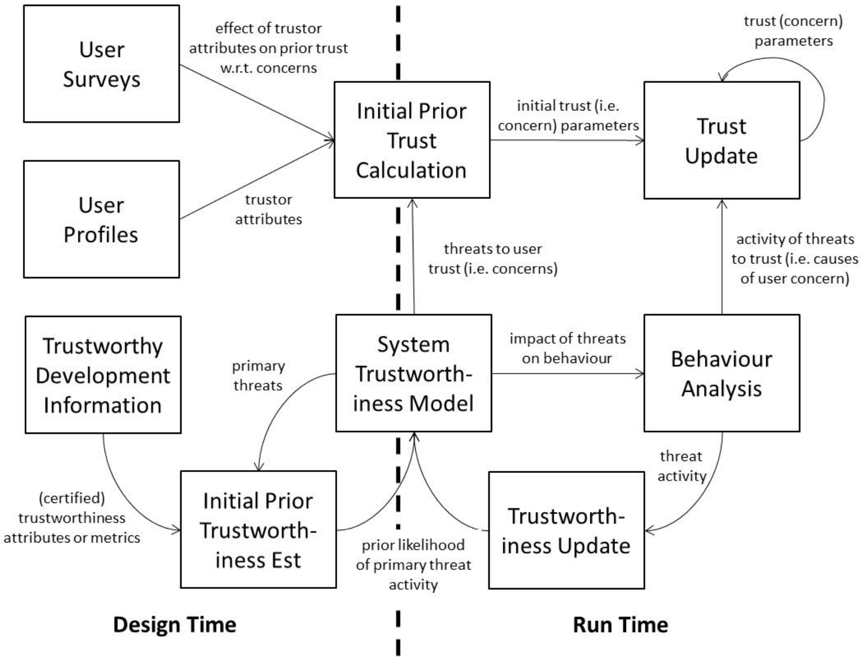

User Surveys
effect of trustor attributes on prior trust w.r.t. concerns
User Profiles
trustor attributes
Initial Prior Trust Calculation
initial trust (i.e. concern) parameters
Trust Update
trust (concern) parameters
threats to user trust (i.e. concerns)
activity of threats to trust (i.e. causes of user concern)
Trustworthy Development Information
primary threats
System Trustworth-iness Model
impact of threats on behaviour
Behaviour Analysis
threat activity
(certified) trustworthiness attributes or metrics
Initial Prior Trustworth-iness Est
prior likelihood of primary threat activity
Trustworth-iness Update
Design Time
Run Time

Figure 1. OPTET WP2 Modelling Approach

At the heart of this approach is a semantic model of system trustworthiness, in which threats to the system are described in relation to groups of interacting system assets.

By using a semantic model, we automate much of the reasoning underlying the OPTET procedures, enabling complex analysis previously done by humans to be applied at composition and run-time. This ensures that:

- system designers do not need so much expertise in how threats might apply to their system because the Generic OPTET model captures this expertise in an applicable form;
- system designers cannot simply overlook or ignore threats from the generic model, making the results less subjective than a conventional risk-based approach.

The model covers socio-technical systems in the Future Internet, in which users are considered to be assets within the system. Situations that may raise user concerns and so potentially affect their behaviour are therefore included as threats in the model. These threats can be used as a basis for defining what is meant by trust (i.e. a belief that the system will address the user's concerns by blocking or otherwise mitigating against these threats). This is a multi-dimensional approach to trust, as the level of belief may be different for each user concern (e.g. a user's level of concern about system availability may be quite different from their concern that a system operator may be fraudulent).
At run-time, Bayesian inference methods can be used to diagnose system behaviour in terms of the activity of all threats in the model, both primary threats (causes) and secondary threats (knock on consequences). This provides a direct estimate of system trustworthiness with respect to a range of potential problems. If threats associated with user concerns are found to be active in the "behaviour analysis" phase, this can be taken as an input to a further Bayesian inference procedure to model the effect on the trust levels of the affected user.

It is important to recognise that most systems (at least most Future Internet systems) are episodic in nature. The system may operate continuously for a long period, but users will interact with the system in a series of usage episodes, each one associated with a set of workflows that is executed over a shorter period. In the Bayesian inference procedures:

- long-term trustworthiness is modelled via the 'prior' probability that each threat is active, i.e. how likely is it that the threat will arise during a single usage episode in the future;
- instantaneous trustworthiness is modelled as the 'current' probability that each threat is active, i.e. making the current usage episode go awry, given the system behaviour;
- user trust is modelled as a set of user beliefs about the long-term trustworthiness with respect to their concerns, i.e. what does the user think is the probability that each of the corresponding threats will become active next time they use the system.

Bayesian inference is used to determine the instantaneous likelihood of threat activity given the long-term likelihood, subject to the evidence from system behaviour. This procedure is used in the 'Behaviour Analysis' step from Figure 1.

Bayesian inference is also used to estimate how a user's experience of previous system behaviour affects their beliefs about future system behaviour. This procedure is used in the 'Trust Update' step from Figure 1.These beliefs are of course subjective, but over time they may become more realistic as the user's experience of interaction with the system grows.

Both long-term and instantaneous threat activity likelihoods are objective measures of trustworthiness [1] [2], based on independent assessments and/or evidence from the system behaviour. Prior to the first episode of use, the expected levels of system trustworthiness can be initialised based on what control requirements are met by the system assets in the "Trustworthy Development Information" step. The expected levels of user trust can be initialised based on the attributes of individual users or classes of users, using survey results to determine how these are correlated with levels of user concern in the "Initial Prior Trust Calculation" step. More details on the WP2 trust and trustworthiness concepts and computations are elaborated in the next two sections.

2.2. Trust

The major objective of our trust computation research activity was to identify socio-technical and economic factors affecting the subjective nature of trust, and formulate them into theoretical models in a mathematical concrete way. To this end we performed two experiments (the DADV experiment and the ACME search engine experiment), both separated into two discrete phases: the involved participants were asked to fill in a questionnaire and additionally engaged with a fictitious online system, observed its functionality and reported their trust level regarding its performance in a separate questionnaire. The purpose of the experiments was two-fold; the first phase allowed us to investigate the personal attributes (social aspects) that cause different trust tendencies among users, while the trust responses related to their interactions with the ACME system endowed us with actual measurements to be utilized for the validation of our proposed models.

More specifically, our research on the social aspects, starting from a literature review and exploratory survey (section 3 and 6, D2.1 [2]) and a segmentation study (section 3.1, D2.2 [3]) isolated three (out of eight investigated) underpinning concepts that have a dominant impact on trust differentiation among individuals, namely:

- "trust stance": the tendency of people to trust other people across a wide range of situations and persons, e.g. trusting someone until there is a reason not to do so;
- "seeking motivation": the motivation to engage in trust-related seeking behaviour, e.g. looking for guarantees regarding confidentiality of the information that someone is providing;
- "competences": competences related to trust, e.g. having the ability to understand one's rights and duties as described by the terms of the application provider.

The repeated findings throughout all the exploratory analyses (section 3.1, D2.3 [1]and section 3, D2.4 [4]) not only motivates but also validates our approach to cluster users into segments of similar trust-related behaviour. Moreover, the ACME search engine experiment also allowed us to expand our findings for each segment towards the nature of their privacy-trust relation regarding disclosing personal information (section 3, D2.4). The following four segments, based on the aforementioned dominant drivers, were distilled out of all this work.

- The *High Trust* (HT) segment displays a so-called high level trust stance. This refers to a tendency of an overall high trust level vis-à-vis (socio) technical systems accompanied by a relative trust in future (legal) measures and other technical safe-guarding. Also several trust-seeking behaviours are present, while a relatively high 'aversion' can be identified for providing certain bits of information. Users in this segment display a rather high interest that such information is not (publicly) available online, underpinned by their available competences to cognitively assess the trustworthiness of online applications and services.
- The *Highly active trust seeking* (HATS) segment can be described by a high level of trust seeking behaviour beyond the mere scanning of trustworthiness cues. Also, individuals seem

to have a higher interest to inform themselves about procedures in case of personal data provision and availability and which may impact their online behaviour to a greater extent than for others. This confirms and strengthens the capacity of possessing a certain competence level that facilitates the assessment of trustworthiness and clues. It also increases the likelihood to address or act upon such events.

- The *Medium active trust seeking* (MATS) segments consists of users with a user experience relatively similar to the HATS. Trust seeking behaviour, however, is less apparent as they seem less preoccupied with (possible risks of) providing sensitive information, or whether this kind of information is publicly (un-)available. In conjunction with this, they are also relatively less inclined to (possibly) change their online behaviour. While the drivers for trust seeking behaviour, such as a relatively low trust stance, can still be detected as well as competences to assess trustworthiness. The motivation to look for trustworthiness clues is still relatively low.
- The *Ambivalent* (A) segment shows a perceived "ambivalence" to assess the trustworthiness of online applications and services. The 'ambivalent' nature of user experience can be explained by a difficulty to cognitively assess trustworthiness and a certain need to trust (according to 'basic heuristics') , such as perceived feelings of loss of control over one's personal information, how personal information is handled and whether current laws and practices are adequate enough to offer protection.

Before proceeding we mention our approach to place trustworthiness in the core of our proposed trust computational models and consider it as a common benchmark for the trust shaping of all segments. Thus, the dominant drivers [1] [4] were further utilized to correlate the trust with the trustworthiness (technical factors) of any system of interest. In particular, we reasonably linked the skills of individuals (motivation and competences) with the accuracy that they perceive trustworthiness, while the under or over-estimation is determined by the level of "trust stance". In other words, we assumed that low levels indicate an overcautious user, while a high trust-stance should result to misplaced trust. We formulated this correlation by means of three compact properties that we expected to appear in the trust-behaviour of segments, as follows:

1. "Highly Active Trust Seeking" users, responded with the higher aggregate values of competences and motivation. Thus, we expect them to assess trustworthiness most accurately compared to any other segment.

2. Users in the "High Trust" segment appear with the highest trust stance among all others. Thus, we reasonably expect them to overestimate the actual level of trustworthiness.

3. All users seem to have adequate level of competences and motivation so as to distinguish between two different systems. In other words, the trust within the same segment is expected to be higher towards a better performing system compared to the trust towards another one with lower trustworthiness.

The expected properties sketched above actually appeared during the two experiments. This fact further validates our segmentation approach and indicates better performance of the proposed models compared to the case of its absence. More details can be found in [4].

For the trust computation, we built on related work and introduced a modified Bayesian inference model as the basis of our approach [1]. More specifically, trust is quantified as the mean of a Beta probability density function, which is characterized by two parameters (α and β). The trust evolution over time is captured by means of these two parameters' update after observing evidence of the system functionality. Our contribution was to extend the followed update process, aiming to attribute specific trust-shaping properties to our proposed models. Recall, that the update of each parameter is a recursive function with respect to its previous value and an update coefficient. Our objective was both to define the form of the function and to compute specific values for the coefficients that reflect actual trust reactions and return accurate trust estimations respectively. Our approach was general enough to be applied for all four identified segments but also for different types of metrics. Thus, we met the core objective of the OPTET project to consider trust as a multidimensional magnitude with respect to the various metrics characterizing the system of interest.
During the second year of the project two mathematical trust models were introduced, both of which followed the common update process to place equal importance on every interaction outcome (e.g. success, failure) independently of the moment that it occurred. This design choice, formulates the property of linear trust evolution and convergence after a relatively large number of observations. Their difference lies in the applied methodology that computes explicit values for the update coefficients: In our first theoretical model we utilized the derived values of the dominant drivers and followed a self-normalizing approach to calculate them. The comparison with actual measurements from the second-year experiment indicates that it achieves to capture the three expected properties, but lacks in accuracy. This fact highlighted the necessity for further evidence, concerning the trust levels. Aiming for more accurate estimations, we designed a "machine-learning" methodology which utilizes a subset of actual trust measurements to compute the update coefficients. In particular, it requires the equality between actual and estimated trust at the initial and two further random time moments. This model clearly outperformed the former and provided trust estimations with acceptable accuracy [4]. We mention beforehand the general form of "machine-learning", making it feasible to be applied independently of the followed update process.
During the third-year experiment, trust responses appeared with severe fluctuations after an outcome interchange, while it had smoother evolution at every common adjacent outcome. The basic "machine-learning" model was proved to be inefficient to capture the pre-described trust shaping (due to the applied update function and the subsequent properties). Thus, we reviewed related work, where authors propose a time-fading mechanism to reflect the behaviour of users who place greater importance on recent outcomes compared to those in the distant past. In technical terms the time-fading effect is captured in the update function by means of the relevant coefficient. Our approach was to further build on related work and provide a variation with the objective to better fit the actual trust reaction. Notice that in this case the "machine-learning" methodology should compute not only the values for the update coefficients but also for the time-fading one. Thus we enriched its functionality with an optimization framework that allows for the identification of unique and optimal values for them. Here again, a comparison with the derived trust responses validates our model which greatly outperformed both related work and our basic one.

We emphasize here the importance of our first proposed model (the one based only on the self-normalized approach), in the absence of actual trust data to be utilized as input for the "machine-learning" approach. Also, it could be used if only a subset of the required input data is available, resulting in hybrid models of the two alternatives.

The economic factors are involved by distinguishing the trust levels form the decisions of users to engage with a system. Note that such a decision should weigh trust with the price and potential benefits or costs from its usage. In [1] section 4.1 we described how a provider may utilize the trust-computational models at the design phase. In section 3.4 of this deliverable, we introduce a respective model for the run-time phase. Thus, our propositions should be considered as a powerful tool on the provider's side, aiming to maximize her potential gains throughout the whole life cycle of the offered system.

2.3. Trustworthiness

In OPTET D2.1 we included working definitions to provide a foundation for our work in WP2 as well as the rest of the project.

> **Trust in a system** was defined as a property of a stakeholder (known as the trustor) reflecting the strength of their belief that engaging in the system for some purpose will produce an acceptable outcome.
> **A system** is composed of assets, each asset representing a physical (including human), organisational or logical component that contributes to its value. System behaviour comprises a set of observable time-dependent properties of the system, which characterize its status and progress towards an outcome.
> **The outcome of engaging in a system** is the end result of system behaviour, at which point a stakeholder could in principle decide whether this result is acceptable, were all relevant aspects known to them.
>
> **A threat** is a situation or event that could potentially arise, whose consequences could alter the system behaviour and lead to an outcome that is unacceptable to some trustor.
>
> **An active threat** is a situation or event that has arisen and is producing consequences for the system behaviour and outcomes.

In OPTET, the evaluation of a specific system asset (or component) is associated with a set of quality attributes that are relevant to achieve its purpose. Thus, trustworthiness quantifies the performance of a component with respect to each particular relevant attribute, by observing its behaviour and measuring what it can actually achieve. These attributes, called "trustworthiness attributes" in D3.1 [6] are clustered into higher-level categories according to the general system property they contribute to. For example, "average response time" is an attribute of the "performance" category.

Based on this approach, we consider the trustworthiness of a component as a vector of the values of all possible trustworthiness attributes. This detailed representation of trustworthiness is aligned with trust, as in the general case, trustors will express their expected system behaviour requirements in terms of different attributes.

A system is more trustworthy if it is able to produce an outcome acceptable to all trustors (based not only on their beliefs, but on their requirements, – thus trustworthiness is an objective property of the system).

In practice, a system becomes less trustworthy when its behaviour suggests that it may be subject to active threats. An active threat does not necessarily lead immediately to an unacceptable outcome, but it indicates that something is happening that threatens the system's ability to avoid such an outcome. This leads to the idea that one can also quantify trustworthiness via the probability that potential threats are active, and hence that the eventual outcome will be unacceptable.

The semantic trustworthiness model developed in the project includes generic assets, threats, controls and misbehaviours. Controls and misbehaviours were derived based on a mapping exercise conducted after analysing the trust and trustworthiness attributes in WP3. A methodology for determining generic threats to the system and a step-by-step approach for creating threat models has been presented in D2.2. Using a semantic model ensures that all concepts are not rendered ambiguous by terminological in-exactitude, even across interdisciplinary boundaries. In the semantic model the terminology is not relevant, as all meaning is captured by expressing the relationships between concepts.

We adopted a layered modelling approach to start with the most basic core model and then specialising concepts as we move down the layer stack with the generic and design-time and run-time trustworthiness models. A generic asset model advancing the state of the art was proposed enabling modelling complex chains of services and service composition patterns. The modelling process has been applied to the different use cases within the project and threats were inferred based on a knowledge base compiled for STS systems. The models were encoded as OWL ontologies to be machine readable and usable by the different components including runtime ones.

Once the system is running, the system behaviour is monitored in order to diagnose problems as they arise. This is done via Bayesian inference technology in WP6 which allows identifying the current likelihood of threat activity and suggests controls to manage them. It also interprets the observations and detects whether there are dependencies between them (primary/secondary threats). This allows for intervention at the right threat with controls that would be effective along the secondary threats chain. The measurement of trustworthiness and threat likelihoods happens in parallel to measuring the trust levels of individual users. The estimated trust levels of individual users can also be used to determine which types of threats users (collectively or individually) are most concerned about, and possibly to control how the system responds to individual users to reassure them when the system is working well, or to warn them of problems they should not ignore should any arise.

3. Trust and Trustworthiness in the OPTET Workflow

3.1. WP3 – Design Phase

Throughout our work in the OPTET project, we highlighted that understanding and grasping the socio-econonomic and legal dynamics underpinning public attitudes to trust in the context of technology and life online more generally, is a key step towards enhancing trust in ICT. In doing so, a better bridge can be made between those who shape technologies and those who consume the technologies.

In line with the stream of thought that focuses on the social shaping of technology, we underline the development of a social view of technological development, rather than following purely techno-centric visions that see technology as the driving force behind social change. This implies that the deployment of a particular technology does not follow directly from the technical properties (or, potentialities) of a new system. Rather, the function, the form, the content, and the uses of every technology are the result of a continuous negotiation within a particular socio-economic and legal context, between various actors such as system engineers, end users, policy makers, and the marketplace.

In this way, users are confronted not with a 'naked' technology, but with one that is already inscribed with certain meanings and uses. However, the adoption and use, or the rejection, of any system by users is the result of their creative re-interpretation within their own experience of everyday life of the uses and meanings inscribed in the system on offer. Following this reasoning, here in OPTET the focus was to yield an understanding of perceived trust drivers and levels in the socio-economic and legal context.

Thus, systems are supposed to reflect relationships of trust, but they are also supposed to support assessment of trust and the development of trust. Considerations related to trust are spread along all phases of system lifecycle, from requirements to decommissioning. Further, there are several stakeholders whose trust has to be taken into account, whether operators or users, companies or the society as a whole. Even the process of design is conditioned on trust within the design team and enabled by collaborative software that builds on trust. Therefore, it may not come as a surprise that the interest in trustworthy digital systems is growing.

For designing trust into online systems it is crucial that software engineering methodologies incorporate what can be seen as objective reasoning and modelling of trust issues in their development stages. In this way software engineers receive assistance in understanding the various trust related issues introduced not only by the system but also from the environment where the system will be placed. It is only then that appropriate design solutions can be identified and implemented. And to this, from our WP2 stance, we have sought to contribute to.

The following paragraph from section 5.1.1 of D2.3 [1] explains the role of the Trustworthy Development Enhancement Toolset (TDET):

> *"The OPTET methodology for trust and trustworthiness management spans both design-time and runtime phases of the STS lifetime.*
>
> *The process starts from the WP3 Trustworthy Development Enhancement Toolset (TDET) that allows the specification of a trustworthy-by-design process composed of building blocks called capability patterns.*
>
> *Trustworthiness-by-Design refers to the collection of methodologies, design patterns, and approaches to realizing the development of systems to be trustworthy. TWbyD methodologies ensure that trustworthiness is at the core of the software engineering*

> *practices so that the entire system and its individual components (standalone or chained) have high levels of trustworthiness through the implementation and maintenance of trustworthiness attributes in the design process.*
>
> *The different GE's constitute tools that support the achievement of the capability patterns (e.g. identification of threats and mitigation controls, measurement of end-to-end trustworthiness, preparing for digital trustworthiness certificates).*
>
> *The output of the TDET is a trustworthy-by-design process handbook customized to the needs of individual organisations, projects and domains. This handbook guides the designer on how to use the different OPTET GE's."*

The Trustworthiness model editor (or SSD) is integrated in the TDET to identify the threats that may compromise the system and thus affect its trustworthiness. Based on a model of the STS and semantic technology the threats from an expert's knowledge base can be mapped to the actual system and instantiated. This provides an objective way for threats identification avoiding errors or misjudgements of the designer. Moreover this can be the basis for the system development by making sure that the suggested countermeasures for each threat are implemented in the system either in the development or the deployment phase. The analysis of the threats and the countermeasures (along with any assumptions) plays an important role for the certification of the system which in turn affects users' trust.

The insights from the segmentation analysis and the resulting construction of the four segments with an identification of the main drivers underpinning trust and privacy highlights towards system developers the diversity among users. When building new applications, the four segments with their respective drivers, competences, attitudes and behaviours allow, on one hand, to make developers aware of various trust and trustworthiness related needs stemming from these different users. In that sense, the segmentation within OPTET led to the inclusion of trustor's attributes in the computational trust model as model parameters. When developing systems, an intake survey thus helps to identify which of the four segments of user experience a user belongs, and to initiate a first model of trust computation with trust values.

System Designers should consider the impact of user personality (e.g., via the outputs of Trust Metric Estimator - TME) for coming up with a profit-maximising combination of trustworthiness levels and price for a software. The optimal trustworthiness level could later be used as an input to the E2E TW Evaluator for evaluating different system options, or finding the minimum trustworthiness requirements for the new software asset.

Assuming that software/system providers are profit maximising entities it is then pretty straightforward that system designers are interested in achieving the level of trustworthiness that will eventually maximise their income minus their costs. However, this is not an easy task.

First of all, their revenues depend on the demand for each combination of trustworthiness level and price. However, this interplay is unknown to the provider, apart from those trustworthiness attributes (e.g., data privacy) and respective metrics where hard laws prescribe the minimum. One of the main reasons is that trustworthiness is conceived differently by different users.

For example, users belonging to the "High Trust" segment would believe that the system is more trustworthy than it actually is. This means that it is very likely that these users will decide to use the software even though they should not. On the other hand, users belonging to the "Ambivalent" segment, who tend to underestimate trustworthiness, may wrongly ignore the software. In order to overcome this problem, in section 4.1 of D2.3 [1] we utilised the Trust Metric Estimator for deriving users' trust level for any chosen trustworthiness level at the end of a trial period. The trial period was deemed necessary for gaining insight about the number of users in each segment and about their valuation[1] and costs of possible outcomes.

Furthermore, increasing the trustworthiness of the software comes at a cost, which can be considered to be a convex function of the trustworthiness level (i.e., the marginal cost is increasing as trustworthiness increases). This cost would include the additional development time, as well as the multi-disciplinary team that should be involved (such as legal experts consulting about restrictions from respective laws).

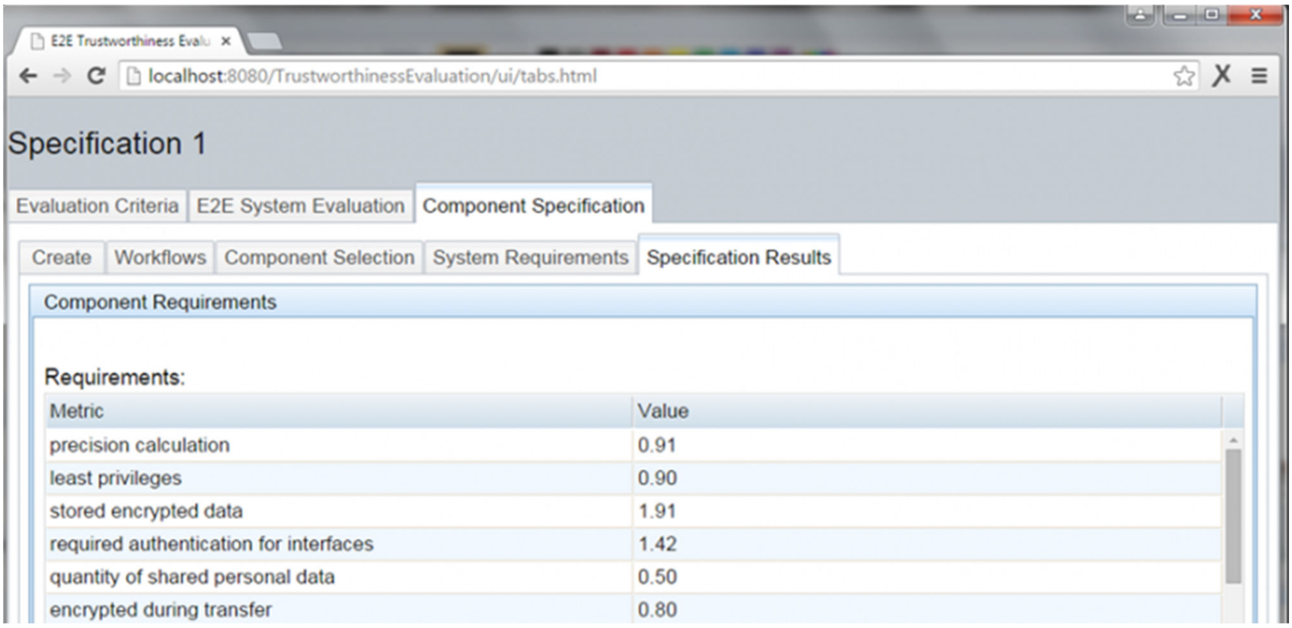
The benefit for the software provider is that they can identify the profit-maximising combination of trustworthiness levels and price. For example, the provider may find it beneficial to target a trustworthiness level that will eventually be accepted by all user segments apart from the "Ambivalent" one. The reason is that users belonging to this segment were observed to underestimate trustworthiness and have the lowest trust level across all segments. Thus, developing software that will be trustworthy enough so that those users' decision process is positive may not be economically viable.

Having established the trustworthiness level that, together with a certain price, will maximize provider's profits, the system designer can then communicate the non-functional requirements to the development team. Those requirements are normalised (expressed as probability values) and thus cannot be directly used by software developers, unless the trustworthiness metric definition provides an explicit mapping to source code properties or measurable software behaviour. For example, a trustworthiness requirement of 0.9 about software availability, which is defined as "sum of functions that use semaphores or mutexes / sum of functions" could be interpreted as "at least 90% of all methods must either use semaphores or mutexes".

This is exactly the case for monolithic software; for composite software that relies on existing off-the-shelf components the system designer would have followed an additional step. More specifically, they should use the E2E TW Evaluator for finding the minimum trustworthiness requirements for the new software asset.

The optimal trustworthiness level for each trustworthiness metric would be provided as an input to the tool, reflecting the global (or E2E) requirement. The following figure presents the trustworthiness specification of a software component to be developed from scratch, which is part of the tools output (namely Trustworthiness Profile). Note that for the following metrics "stored encrypted data" and "required authentication for interfaces" the target value is greater than 1. In such cases (or when the target is lower than 0), the end-to-end target value cannot be met with the specified configuration. In that case, the system designer can try selecting a different set of existing software instances; e.g., more trustworthy in terms of the unsatisfied metrics.

[1] According to the Multi-dimensional trustor's decision criterion presented in Section 4.1.1 of D2.3 [1], users' valuation will affect their decision on whether to use the software, or not, because when adjusted by their trust level it should be greater than the price asked to pay.



Specification 1

Component Requirements

Requirements:

Metric	Value
precision calculation	0.91
least privileges	0.90
stored encrypted data	1.91
required authentication for interfaces	1.42
quantity of shared personal data	0.50
encrypted during transfer	0.80

Figure 2 - E2E Trustworthiness Calculator showing an asset Trustworthiness Profile

In addition to the computation of the trustworthiness metrics for the selection of a new asset, the threats and control objectives should be taken into consideration. The WP2 GE SSD provides this information (threats and control objectives) per asset. This guides the designer in the selection process balancing cost versus risk. Note that the control objectives can be actually implemented in different ways allowing flexibility in the choice of the implementation technology based on the system's economic, social or regulatory context. The regulatory aspects are presented in more detail in section 4.

3.2. WP4 - Development & Certification Phases

From a user perspective, the importance of trust seals and legal cues was highlighted in our work. In particular the trust-privacy survey in the fictional ACME search engine pinpointed that a vast majority of users look for information about the reputation of an organisation in order to assess the trustworthiness. However when an ICT platform is quite unknown/unfamiliar to a user, and lacks distinguishable characteristics or explicit information, an information asymmetry arises as users are without access to relevant underlying socio-economic, technical and legal information, and the necessary interdisciplinary knowledge bases required to make a robust trustworthiness assessment.

In order to increase trust and adoption of an IT solution, our work thus highlights the need for taking into account various signalling methods to better communicate trustworthiness attributes to end users: openly releasing notices, terms and conditions, codes of conduct, membership of authorative organisations, (industry) awards, certificates, policies, informed consent, click-wrap licences and certification/trust marks/seals. The segmentation analysis highlighted that these legal cues are perceived to be useful, with only a small minority (9%) never looking for such guarantees. Especially, in this phase of development or certification phases, our work highlighted that trust marks are gaining in importance in signalling trustworthiness since the majority of respondents reported to always or sometimes look for them and were cautious about visiting or using online services, systems or applications without them. In this respect, our work highlights the need for the OPTET workflow to be attentive to trust marks from public regulators (such as for example EMOTA or EuroPrise) as they are perceived by users as being more authoritative than others. Trust marks/seals are thus also becoming bound up in a hierarchy of authority and towards this aspect as well as that different users understand trust makers differently, online platform, service or application providers should become attentive to.

Secondly, it remains unclear to what extent users fully appraise, acknowledge and understand legal signposts as for example in our segmentation questionnaire the majority respondents (65.9%) reported to use Google but not having read its privacy policy. And on the aspect of understanding, there is the problem regarding users who perceive themselves to be legally-aware and possess indeed sufficient legal understanding and those who claim to be legally-aware but in reality have insufficient legal understanding. Thirdly, it became apparent that end users, if they look for legal information, look for certain legal cues, in particular liability. Further research is more than needed on these aspects, but nonetheless pinpoint for the need of platform, service or applications providers to take into account aspects of perceived usefulness regarding end-users when elaborating their legal signposts and try to work this to redress some knowledge asymmetries. For example, a way can be to tailor these popular cues in such as a way as to include other important but less searched for legal information.

Finally, our work highlighted that legal signpost methods signalling untrustworthiness, such as notifying users of a data breach incident, still needs more strengthening since a majority of respondents claimed not be able to detect when their personal data has been misused or when a third party has gained access to an application without authorisation. Although in some instances a mandatory notification of untrustworthiness is a legal requirement, this is currently limited.

From an end user perspective, we can thus conclude that there exists an imbalance between the awareness and use of legal trustworthiness cues and signalling untrustworthiness. Both dimensions should be taken into account in order to allow end users to make fully informed decisions and increase legal awareness. Moreover it is impossible to eradicate all trustworthiness breaches. In that context, for an organisation, transparency over untrustworthiness might be a preferred strategy: it could enhance its reputation by demonstrating that it takes data breaches seriously by showcasing how it tackled it. This strategy is also worthwhile, as a number of users will continue to utilise a platform even after a known data breach has occurred.

Rather than relying solely on subjective knowledge or overlooking legal issues entirely, a better approach would thus be that designers objectively identify relevant trustworthiness attributes; designers and developers of ICT platforms are forced to embed these attributes at the earliest point of time; data controllers using these platforms adopt adequate technical and organisational measures to ensure these trustworthiness attributes are effective; and, these measures are signalled to end-users at a later stage – through legal cues such as trust marks.

Based on the specification of trustworthiness requirements contained in the trustworthiness profile, the system designer can monitor the quality of the software module being developed and whether it is ready for release, e.g., to a marketplace.

Furthermore, in section 4.2 of D2.3 [1], a theoretical model is described arguing that a marketplace operator could play a more active role in the certification process. More specifically, we investigated a business model for the marketplace operator who wants to differentiate from competing platforms by offering more accurate information about the trustworthiness of the listed products to its users.

When a product version becomes available to the OPTET trustworthy marketplace, the operator attaches (next to it) a digital trustworthiness certificate issued by a certification authority. Such a certificate can greatly help buyers choose the most appropriate product. These certificates include the countermeasures implemented in the solution in response to identified threats. There are cases however where such certificates alone are not enough for users to trust offerings to the level that reflects their actual trustworthiness.

Imagine for example a situation where two different certification authorities exist, which use different metric definitions in their computations, or varying approaches for calculating trustworthiness attributes. In that case the resulting trustworthiness metric/attribute values will probably be different and the marketplace operator would have to take some further action to help users. A suboptimal option for the users would be to discard a certificate randomly. Other candidate options requiring more effort from the provider would be to consult a third certificate provider hoping that any two certificates will be (almost) identical, or even to inspect the metrics/attributes used and select one of them to include.

Another case is that the certificates may be limited to design-time metrics only, making users less confident that the product will meet their requirements at run-time. The marketplace provider could wait until a sufficient number of early adopters use it and provide their own ratings, but this option has four main drawbacks.

1. In the meantime the majority of users will be choosing other products which could be less trustworthy.
2. There is always the possibility that the new product will not succeed during the first trials and thus the rest of the users will be discouraged to use it any more, even though its actual trustworthiness could be higher than any other competitive product in the marketplace[2].
3. Early adopters should be willing to share their actual experiences with the rest of the users; an assumption that is less realistic when marketplace users are service providers who compete for customers. This means that such "selfish" users would either choose to manipulate this information or not upload it truthfully to a public repository at all. Unless the marketplace operator has imposed restrictions on who has access to the collectively achieved knowledge, this information can be considered as a "public good". More specifically, the derived information can be utilized by all users regardless of their contribution to the public fund. The non-excludable nature of such good leads to free-riding behaviour, meaning that any rational user would be willing to minimize their funding contribution.
4. Finally, the optimal number of experiments depends on the utility of the users, which is private information. If all users were free-riders (reported an extremely low utility) then each one would have to perform the necessary number of experiments on its own. But this cost could be prohibitively high for any individual user, in which case the society may fail to identify the product's actual trustworthiness (because not enough trials were performed). But, even if users can pay for that this is obviously an inefficient outcome.

Thus, the marketplace operator has to incentivise users to truthfully report their utility in order to decide the optimal number of experiments that have to be performed. The problem of incentivizing users to truthfully report their utility could be dealt with well-known Vickrey-Clarke-Groves (VCG)

[2] The product’s ability to perform well can be seen as a random variable following the Bernoulli distribution.

charging scheme. But, this may also require that policy makers contribute as well (so that the mechanism is "budget balanced").

3.3. WP5 - Distribution and Deployment phases

A system designer can upload the software being produced to the marketplace and set the price according to the suggestion of the theoretical model.

A marketplace addressing the distribution and deployment of trustworthy solutions should itself be trustworthy (for instance it should have controls that prevent attackers from compromising the integrity of published software or any textual description of it). This means that the guidelines for trustworthy systems design described above are relevant for the design and deployment of the marketplace itself. This includes the trust aspects given the targeted categories of the users and stakeholders of the system as well as threat analysis to identify any issues that may compromise the trustworthiness of the marketplace and possibly solutions bought or deployed through it.

A Marketplace operator can also help the users in the software selection proceess by integrating the E2E TW Evaluator into its platform utilising the programming interfaces made available. For example, the OPTET Trustworthy Marketplace offers a recommendation service that invokes the E2E TW Evaluator in order to evaluate how closely different configurations match the profile of a certain user.

Similarly, a product manager in charge of finding the suitable system configuration for a service provider can use the E2E TW Evaluator for comparing the trustworthiness levels of different options to the optimum required one. This can be done either by invoking the E2E TW Evaluator directly (assuming that a provider offers such a service) or indirectly via Marketplaces.

3.4. WP6 - Maintenance phase

The service provider should maintain trustworthiness level of a system at run-time, by taking customer expectations and operational costs into account across the entire lifecycle of a system (i.e. from design and development to maintenance phases). Monitoring trustworthiness perceptions and trust levels of users remains important in the light of changes in the service due to new business opportunities or new technical possibilities and users themselves might change due to contextual or personal factors. This is very important for delivering better service quality to users, increasing market share by gaining users' trust, mitigating adverse effects and keeping costs under control through efficient resource allocation. However, achieving this balance is not an easy task for the following reasons. The retail provider has no perfect information about the actual trustworthiness of each individual component/service instance and the customer expectations are usually unknown.

The provider could compare the trustworthiness of candidate components by querying a marketplace that carries detailed trustworthiness certificates, such as the OPTET Trustworthy Marketplace. Furthermore, the provider could offer SLAs (Service Level Agreements) where the exact trustworthiness levels are described as a set of metrics and their respective target values. Then we could assume that the user would not trust the provider again in the future if any threshold value was not met. In the following sections, however, we will assume that the retail provider does not want to offer SLAs.

Furthermore, we will assume that the user will interact with the provider's system several times and the number of transactions is known in advance (i.e., is the only term of the contract). For example, consider a bank manager that wants to process all saving accounts (e.g., calculate interests etc.) at the end of the day and enters into a monthly contract with a cloud computing provider. Whenever the service provider believes that the customer's trust is lower than a certain threshold the former could make the necessary changes to the system in order to try regain the customer's trust after a few transactions. The optimal changes that should take place at any point in time are based on a finite-stage dynamic programming model, which has been adapted so that changes are restricted by the available components (instead of assuming that trustworthiness is a continuous function of effort which is more suitable for services offered by humans). In order to estimate the current user's trust level we employ the trust computational model of the TME, which has been described and validated in [1].

3.4.1. The Trust Computational Model

Suppose that the provider offers a single service plan to all interested buyers, which allows them to place a fixed number of n transactions for an upfront payment p_s, or unit price $p = p_s/n$. All candidate customers, being rational entities, will investigate whether they should engage with that provider, or not (the interested reader is redirected to [1] for a detailed decision criterion). If multiple providers exist in the market then obviously each customer would select the one that maximizes her expected net benefit. First-time buyers will not have experienced any system outcome before and thus their initial trust metrics ($\tau_i^j(0)$) would depend on their personality (e.g., predisposition) and any information that they can find in service description, or from their peers. For simplicity, in the following we will assume that a single binary trust metric j is important for the system only and thus the overall trust at any time is given by $\tau_i = \tau_i^j$.

Let us assume that a certain customer i has found this service plan to be beneficial. After making the upfront payment, the customer answers a questionnaire that helps the provider to identify the trustor's segment, see 2.2. This would allow the provider to use the trust computational model to compute the initial trust metrics. This value could be considered as a safe, minimum target for the overall trust (or respective trust metric in the general case) after n transactions in order for the trustor to renew the business relationship. The rationale is that *ceteris paribus* the user's decision would be positive if its trust level after n transactions will not have decreased.

The next step would be to compute k, the minimum number of successes necessary for reaching the initial trust level. Again, the complexity of this step can be significantly reduced by relying on the mechanics of the trust computational model. More specifically the minimum number of successes can be computed by solving the following equation for k:

$$\tau_i(0) = \frac{\alpha_0+\alpha*\mathrm{K}}{\alpha_0+\alpha*\mathrm{K}+\beta_0+\beta*(n-\mathrm{K})} \Leftrightarrow K = \frac{\tau(\alpha_0+\beta_0+\beta n)}{\alpha-\tau(\alpha+\beta)} \qquad (1)$$

The last step is to create a contingency plan for reaching the initial trust level in the most cost effective way, or abandon serving the customer as early as possible. This contingency plan would suggest to the provider the optimal level of system trustworthiness at any possible situation. A situation is characterized by the tuple (number of successful transactions still necessary, number of transactions remaining). Obviously, such a contingency plan requires that the provider is able to make the necessary changes to system trustworthiness between two consecutive transactions. For example, in case of a composite system the provider could replace a component with another one and thereby obtain the target trustworthiness value. In case of a monolithic system the trustworthiness could be affected by a different configuration. We should note that usually different system compositions, or configurations, entail a change in provider's costs. Furthermore, we would expect that increasing a component's trustworthiness is costly for its developer, e.g., a component's cost in the market equilibrium is an increasing function of trustworthiness.

Thus, the provider has received p_s monetary units in advance and knows the conditions for securing that revenue stream in the future. Suppose that the provider can query an online application marketplace and find information about the trustworthiness t_m and cost c_m of any component m that is compatible with the rest system. At the beginning or at state (k, n) the provider has two main options:

1. Serve the customer and hope that the service will be trustworthy enough for getting an extra amount p_s for the next set of transactions.
2. Keep the money and do nothing.

Depending on the trustworthiness level $t_s\widehat{(k,n)}$ of the system s chosen at state (k, n) there are two cases:

- With probability $t_s\widehat{(k,n)}$ we go to state $(k-1, n-1)$
- With probability $1-\widehat{t_s(k},n)$ we go to state $(k, n-1)$

The same options are valid at any later state apart from the following situations:

- (k^-, n^+) where $k^- \leq 0$, $n^+ > 0$ and the provider has no incentive to keep placing effort, since effort is costly and would not further increase its future revenues.
- $(k^+, 0)$ where $k^+ \geq 0$ and the provider will have exhausted the number of attempts before satisfying the customer.

Thus, the run-time provider's problem can be phrased as "what is the most cost-effective trustworthiness level for the next transaction given the total number of transactions remaining and the minimum number of successes required to meet the customer's expectations?".

Such a problem can be solved by employing a finite-stage dynamic programming model, like the one described in [5]. This contingency plan can be produced proactively and be used by the provider to take any corrective actions deemed necessary at run-time. Note that the contingency plan suggests a trustworthiness level for the overall system. In the case of a composite service for example, the provider would have to replace a subcomponent with another one (or add a new) so that that the overall system meets the new security level. This is not a trivial task, but the provider could rely on tools that allow estimating the end-to-end trustworthiness of a particular system composition, like the E2E TW Evaluator as described in Section 3.3.

Similar to [5], let $V_n(k)$ be the minimal expected cost incurred when the provider is at state (k, n), which refers to the path on the tree shown in Figure 2 below with the minimum total remaining expected cost. Then the provider's maximum expected profit π^* is given by $\pi^* = 2p_s - V_n(k)$. The first term represents the maximum revenues that the provider can receive in this 2-period setting, while the latter includes both the operating costs, as well as, any missed opportunities.

Furthermore, assume that:

- $V_0(x) = p_s$, where $x > 0$, which means that the provider misses the opportunity to renew the contract with the customer, and
- $V_y(x) = 0$, where $x \leq 0$ and $y \geq 0$, which means that there is no "penalty" when the minimum number of successful transactions is met.

Then, the Bellman optimality equation for this problem can be written as

$$V_n(k) = \min_{p_s \geq c \geq 0} \left\{ c + t_s\widehat{(k,n)} V_{n-1}(k-1) + \left(1 - t_s\widehat{(k,n)}\right) V_{n-1}(k) \right\}$$

where $c = \sum_m c_m$ is the total cost and we would expect that the provider considers system compositions/configurations whose total cost does not exceed the retail price.

This dynamic programming model is equivalent to the one studied in [5]; the only difference being that there is no SLA between the two parties and thus the penalty refers to the missed opportunity for receiving another upfront payment. Since the upfront payment p_s is fixed, the condition $\mathrm{V}_0(\mathrm{x}+2) - \mathrm{V}_0(\mathrm{x}+1) \geq \mathrm{V}_0(\mathrm{x}+1) - \mathrm{V}_0(\mathrm{x})$ is still satisfied and the optimal policy that was found is still valid. Thus, in general, the contingency plan would instruct the provider to do the following:

1. Increase the TW the closer we get to contract's end and the minimum number of successful transactions was not reached. Furthermore, the higher the number of pending successful transactions the higher the increase of TW would be.
2. Decrease the TW as the number of pending transactions to reach a certain number of successful transactions increases. Furthermore, the higher the number of pending transactions the higher the decrease of TW would be.

Note that, for simplicity, the contingency plan is assumed to be used for finding the optimal design-time trustworthiness $t_s\widehat{(k,n)}$ for that particular user, or segment in general. Contingency plans computed by the OPTET Optimal Control Selector can take into account not only multiple customers using the same system, but multiple systems relying on a certain software module.

Finally, the provider would have to prepare one contingency plan for every trustworthiness metric $j \in H_s$. The computational complexity of producing such a contingency plan is $O(\frac{n(n+1)}{2}|m|)$, where n is the number of transactions and $|m|$ is the number of candidate components. In order to see this remember that the dynamic programming problems inherently support recursion and thus the total number of states is given by a finite arithmetic series, $1 + 2 + 3 + \cdots + (n+1)$ (as shown in **Figure 3**). Furthermore, in each state we have to compute $|m|$ expected costs in order to find the minimal (assuming that $m = 1$ refers to a dummy component representing the "do nothing" strategy).

3.4.2. An example

Suppose for simplicity that the provider can manage system trustworthiness by replacing one component with another from the marketplace, while the rest components are proprietary. The following table presents the cost c_m per transaction and the trustworthiness t_m of each candidate component (again we focus on a single trustworthiness metric), where $m = 1$ refers to a dummy component representing the "do nothing" strategy.

Table 1. Candidate components

Component m	1	2	3	4	5
Cost c_m	0	0.3	0.4	0.8	1.9
Trustworthiness t_m	0	0.54	0.6	0.8	0.85

Furthermore let us assume that the offered service plan covers 4 transactions for an upfront payment of 3 monetary units; thus $n = 4$ and $p_s = 3$. If the customer, upon registration, had answered a questionnaire for revealing the trustor segment and it was found that she belongs to the "High Trust" segment, then her initial trust level would be $\tau_i(0) = \frac{\alpha_0}{\alpha_0+\beta_0} = \frac{2.2144}{2.2144+0.7106} = 0.7571$. Thus, in order for her trust level after 3 transactions to be >=0.7571 the provider would have to succeed in at least $\lceil k \rceil = \lceil 2.35424 \rceil = 3$ transactions, where k is given by equation (6) or more specifically:

$$\frac{2.2144 + 0.9583 * k}{2.2144 + 0.9583 * k + \ 0.7106 + 0.4399 * (4 - k)} = 0.7571 \Leftrightarrow k = 2.35424$$

Figure 2 presents the contingency plan that would be produced in this example. Solid lines represent the trustworthiness of the optimal component that should be selected, while the dashed line gives the transition probability to a state where the remaining number of successful transactions remains the same. Rectangles denote a final state and any missed revenues. Note that during the first two transactions the provider should employ $m = 2$. Furthermore, at state $(1{,}1)$ the provider would maximise its expected profits by using $m = 4$ that has increased trustworthiness and cost. Finally, note that whenever the provider realizes that, either the minimum number of successful transactions cannot be met, or it has already been achieved, then the optimal component is $m = 1$ (doing so reduces costs without affecting future revenues).

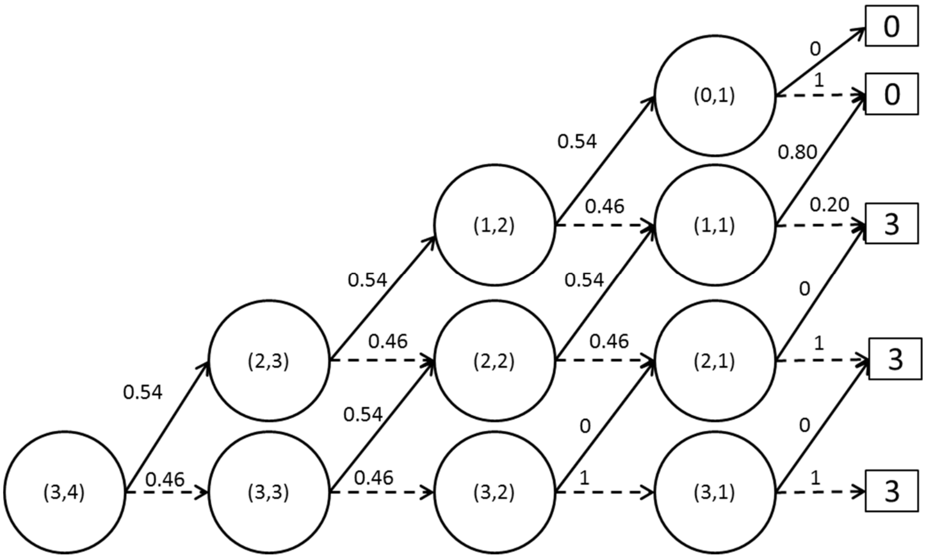


Figure 3. An example of the contingency plan

The maximum expected profit is $\pi^* = 2 * 3 - V_4(3) = 6 - 2.72028 = 3.277972$. To see why this problem is not trivial, let us examine the following two extreme cases. The first option of the provider would be to place no effort at all. In that case the provider's expected profit during the two phases would be $\dot{\pi} = 2 * 3 - V_0(3) = 6 - 3 = 3$ (the upfront payment of the first phase, only). The other strategy would be to employ the most trustworthy component so that the customer will have observed the maximum number of successes and the probability of renewing the contract is maximized. However, c_5 is so high that the total expected cost is higher than the missed opportunities from further revenues; more specifically $\ddot{\pi} = 2 * 3 - V_0(-1) = 6 - 3.99009 = 2.00991$.

3.4.3. Trustworthiness maintenance

Trustworthiness is maintained in WP6 by monitoring the infrastructure and detecting any threat activity. The detection is based on the following information:

- The threat set that have been encoded in the *Design-time trustworthiness model* as well as the associated controls.
- The misbehaviours associated with the threats also encoded in the *Design-time trustworthiness model*.
- The link between the misbehaviours and monitored metrics. This link is produced during the metric engineering process. It defines when a misbehaviour is happening based on the value (or value change) of metrics.

The detection uses the Bayesian inference in order to infer threat activity from observed misbehaviors. A single misbehaviour can affect the probability of multiple threats being active.

When either a trust concern or a trustworthiness threat is considered to be active, the Mitigation GE will be directed to activate a control. The exact control to be applied would be semi-automatically chosen by the Control Identification and Selection component of the trust and trustworthiness maintenance tool and the administrator. More specifically, based on the above probabilities an administrator could be supported by the Control Identification and Selection in selecting the most appropriate control objective and control type. In case a software mulfunction misbehaviour for example reached the Trustworthiness Evaluator, the selected control objective could be asset replacement. Similarly, sending a technician instead of remote software patching could be chosen as control type. Finally, for the selected control type multiple options may be available (for instance from different software vendors) and the Control Identification and Selection could automatically choose the most cost-effective one to be activated.

When choosing the most cost-effective control there is a trade-off that must be considered between the cost of deploying a certain control and its effect on user's trust and eventually on revenues. It is exactly this trade-off between trust and trustworthiness that needs to be balanced. A provider having an estimation of the user's current trust level (either from the Trust Metric Estimator or the Trust Estimator) can predict the expected new trust level after the outcome of the on-going transaction is evidenced. Then, the provider could compute the minimum trustworthiness level of a control that should be selected in case of a misbehaviour. In that way the provider can prune some candidate controls and ideally find the control that would maximise her expected profits in the next period. The optimal trustworthiness level computed before could be used as an input to the E2E TW Evaluator for evaluating different system options, or finding the minimum trustworthiness requirements for the new software asset, closing the loop from run-time to design-time.

4. Towards improved legal integration within a developing Future Internet environment

Section 4 focuses on the possible future legal measures that are likely to have a role in the overall approach to a trusted Future Internet. This section specifically draws attention to the legal aspects of a value-by-design approach and addresses the following primary research question:

4.1. Research question and contribution

'What is the role of the law in a value-by-design approach to a trusted Future Internet environment?'

The key rationale behind the OPTET project is to reduce trust erosion in a digital age: (i) through better-understanding the significant socio-economic, legal and technological aspects of trust and trustworthiness; and, (ii) by utilising this interdisciplinary knowledge to inform the development and provision of technologies that enable evidence-based trustworthiness management for key stakeholders to utilise (in order to design and develop trustworthy ICT platforms). The success of the OPTET project predominantly lies with its diverse team of experts engaged through an ongoing interdisciplinary dialogue.

In contrast to many current systems, services and applications providers, OPTET asserts that trustworthiness should not be an afterthought or add-on. Rather, trustworthiness should be embedded into the whole lifecycle of an ICT platform starting from the earliest point of its design and development; i.e. from cradle-to-grave or cradle-to-cradle. This is known as trustworthiness-by-design (TWbyD), which is defined in the OPTET D3.1 Report [6, p. 22]:

Trustworthiness-by-design (TWbyD): is a collection of methodologies, design patterns at architectural level, and approaches to realizing the development of systems to be trustworthy. TWbyD methodologies ensure that trustworthiness is at the core of the software engineering practices so that the entire system and its individual components (standalone or chained) have high levels of trustworthiness through the implementation and maintenance of trustworthiness attributes in the design process. Conversely, TWbyD also offers rigorous definitions of **trustworthiness attack patterns.**

Francesco Di Cerbo et al. [7] further describe the TWbyD concept:

"*As a consequence, we speculate that by selecting a relevant set of attributes in the early development life-cycle of the system, it is possible to design it in a way so that there will be mechanisms to ensure, evaluate and monitor trustworthiness. We call this trustworthiness-by-design (TWbyD), and the idea that trustworthiness must be considered in all development phases and built into the core of the system rather than bolted on as an afterthought. TWbyD is a collection of reusable development process building blocks that can be added to existing software engineering methodologies.*"

TWbyD belongs to a wider grouping of value-by-design approaches, which intentionally plan to incorporate chosen types of principles (e.g. trustworthiness and privacy), standards of behaviour and their attributes across ICT platform design and development.[3] One of these other value-by-design approaches – data-protection-by-design (DPbyD) – is set to become a legally-binding requirement under Article 23 of the proposed European General Data Protection Regulation (GDPR) [8].[4]

Section 4 therefore aims to explore the **possible role of value-by-design**, as a legal measure, in the overall approach to a trusted Future Internet environment by critically assessing these two approaches – **trustworthiness-by-design** (**TWbyD**) and **data-protection-by-design** (**DPbyD**) – through **cross-comparative evaluation** (see sections 4.4 and 4.5). As a result of this critical analysis, this section **identifies a need for greater legal integration** across the ICT platform lifecycle in order to strengthen a value-by-design approach to a trusted Future Internet environment. In consequence, it **proposes the OPTET Legal Integration Model (OPTET-LIM)** aimed at raising legal awareness and interdisciplinary exchange from the ICT platform design stage (see section 4.6). Finally, it briefly explores the newest legal instrument that explicitly aims at promoting trust online – **the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) Regulation** – including its connection to value-by-design (see section 4.7) and explains why a TWbyD approach is crucial in such an environment.

This cross-comparative evaluation is achieved through critical assessment of the proposed legal framework for DPbyD.[5] While the DPbyD approach should be welcomed (as it is potentially applicable to all future ICT platforms), it appears to have various weaknesses (see section 4.4). For instance, Article 23 imposes the DPbyD obligation on controllers (i.e. the users of the technology) rather than system developers, system designers, and other key stakeholders that directly influence the overall configuration of an ICT platform. Furthermore, it is unclear what Article 23 expects from data controllers: compliance with technical standards (embedding legal rules) and/or implementation of technological measures?

Value-by-design implementation requires a reliable evidence-base and rigorous review. In legal terms, organisational-level (and where possible independent) evaluation of ICT platforms is required to ensure that a particular platform, at the bare minimum, complies with legal obligations. Therefore, as part of this cross-comparison, Section 4 also examines three legal awareness models that could be (potentially) used for this scrutiny: (1) legal compliance checks; (2) data protection impact assessments – under Article 33 of the GDPR; and, (3) certification – under Article 39 of the GDPR.

In the context of DPbyD verification, data protection impact assessments (DPIAs) are usually carried out. However, DPIAs do not guarantee an on-going interdisciplinary dialogue and accountability – two key grey areas for successful value-by-design implementation. Therefore, in response to these two key grey areas highlighted within the proposed legal framework, Section 4 identifies a pragmatic need for better legal integration[6] within the ICT platform development lifecycle and thus puts forward

[3] Cory Knobel and Geoffrey C. Bowker [61, p. 26] state: *"[e]xamples of existing work in along this theme include Batya Friedman's values-sensitive design, Mary Flanagan and Helen Nissenbaum's Values at Play, Phoebe Sengers' reflective design, T.L. Taylor's values in design in ludic systems, and Ann Cavoukian's privacy by design".*

[4] Based on the similar privacy-by-design (PbyD) approach; see Section 4.4 for full information.

[5] Refer to 'Table Two: GDPR, Article 23 draft versions' and 'Table Four: GDPR, Article 33 draft versions' in the Annex for all three draft text versions released by the European Commission, European Council and European Parliament.

[6] This report defines 'legal integration': a state of being well-informed about the status, substance and implementation of pertinent soft and hard legal measures (in force and/or pending enactment) throughout the ICT platform lifecycle. It is

the OPTET Legal Integration Model (OPTET-LIM) described in section 4.6. The OPTET-LIM recognises that key stakeholders need to be well-informed about pertinent legal measures throughout the platform lifecycle. This model is aimed at raising legal awareness and interdisciplinary exchange from the ICT platform design stage. OPTET-LIM maps these legal integration requirements onto OPTET's "Trustworthiness Application Lifecycle". Section 4 therefore aims to: (a) demonstrate that TWbyD is well-suited to establish a trusted Future Internet environment; and, (b) emphasise the need for improved legal integration – through OPTET-LIM – within trustworthy application design, development, certification, distribution and deployment, and maintenance phases.

Section 4 builds on previous work in D2.1 and D2.4 conducted by iLaws, which focused on **the interplay between the law and trust**. The OPTET D2.1 Report examined the function of the law within trust optimisation, and legal definitions of trust [2, pp. 22-34]. The Annex to this report [2, pp. 144-167] also highlighted a number of significant existing legal measures across three areas pertinent to online trust: (i) contract law, (ii) data protection law, and (iii) information security law. In addition, the OPTET D2.4 Report explored the pragmatic effect of legal awareness on an individual's perceived level of trust. However, both D2.1 and D2.4 found the interplay between the law and trust to be unclear. By drawing on a key conclusion raised in D2.4 – that trustworthiness should be at the core of a legal strategy in an overall approach to trust optimisation – this section now moves on to examine **the interplay between the law and trustworthiness**.

In summary, Section 4 is divided into four parts. In view of the research question, Part I first sets out to briefly identify how a potential 'Future Internet' environment is defined and envisioned (see section 4.2) and the possible challenges it may pose to current regulatory frameworks (see section 4.3). Part II then explores the interplay between the law and trustworthiness in the context of value-by-design via cross-comparison of TWbyD and DPbyD approaches (see section 4.4) and their evidence-bases e.g. DPIAs and OPTET-LIM (see sections 4.5 and 4.6). Part III briefly examines the eIDAS Regulation [9] and its connection to value-by-design (section 4.7). Part IV concludes this section by addressing the research question (bringing together Parts I, II and III) and outlining key areas for future work (see Section 5).

4.2. 'Future Internet': brief overview

The concept of the 'Future Internet' lacks a precise, agreed definition and a single vision for its practical development [10, p. 249].[7] The European Commission [11] outlines its view of a Future Internet as follows:

"There was a time when connecting to the internet meant being tethered to a desk and chained down by cables. […] [/] Research projects funded by the European Commission are spearheading future networks which are fast, flexible and ever-responsive to demands from both humans and machines for access to content, apps and services relevant to the context and location of the user. This is how the future internet is evolving: as an internet of services, things and infrastructure. From smart appliances that talk to each other to clothes that monitor our health; from cars that cannot crash to mobile technologies and cloud platforms that run our businesses."

built on robust: (1) interdisciplinary dialogue which involves (a) good communication and (b) sufficient legal understanding; and, (2) audit trail.

[7] For instance, the Internet Society (ISoc) [178] – an international organisation promoting internet policy, standards and development – provides a number of alternative Future Internet scenarios on its website. Also see [179] for further information.

The literature also provides two useful definitions for the Future Internet. Firstly, Eddie Townsend [12, p. 2] offers the following description:

"The Future Internet: [/] *An evolving convergent Internet of things and services that is available anywhere, anytime as part of an all-pervasive omnipresent socio–economic fabric, made up of* ***converged services****,* ***shared data*** *and an advanced* ***wireless and fixed infrastructure*** *linking people and machines to provide advanced services to business and citizens."* [Bold emphasis in original document.]

Secondly, Mauro Caporuscio and Carlo Ghezzi [13, p. 9] advance a further definition:

"The Future Internet is envisioned as a worldwide environment connecting a large open-ended collection of heterogeneous and autonomous resources, namely Things, Services and Contents, which interact with each other anywhere and anytime. Applications will possibly emerge dynamically as opportunistic aggregation of resources available at a given time, and will be able to self-adapt according to the environment dynamics."

The Future Internet concept is a means of constructing a plausible representation of a maturing digital age. Despite the lack of a clear-cut approach, this matured digital environment is one characterised by greater and more seamless device connectivity, and increased data generation, sharing and re-usage across multiple ICT platforms occurring between: machine-to-machine, machine-to-person and person-to-person. This view of a Future Internet is also seen as a shift away from the host-centric networks of the early Internet to more user-centric and context-aware networks [14, p. 280]. While it is not possible to fully outline the scope of the Future Internet, the Internet of Things and cloud computing both appear to be integral aspects of this vision and, to a certain extent, are already in operation.[8]

4.3. Possible future legal measures: brief overview

4.3.1. 'Future Internet' and its legal inheritance

There are three significant ways in which the Future Internet environment is likely to change the collection and processing of (personal) data, through: (1) a higher volume of data, and increasingly sensitive data types, generated through a multitude of (interconnected) devices; (2) the opportunities for increased interoperability, aggregation, analysis and interpretation of (personal) data from numerous sources; and, (3) the increased speed and ease in which these (personal) data are collected, processed, copied and shared.

This raises two crucial questions for those considering the possible future legal measures that are likely to have a role in the overall approach to a trusted Future Internet: (a) do these alleged 'new' challenges posed by a Future Internet environment constitute either a complete departure from or re-manifestation of past issues experienced within the pre-digital age and digital age (thus far)? (b) Do these alleged 'new' challenges posed by a Future Internet environment therefore necessitate new forms of governance or will existing legal obligations suffice? In answer to these questions, it is a misconception to presuppose that all present legal measures will in some manner require complete and radical transformation to remain relevant within a maturing digital age. After all, concepts such as data protection, privacy and security are central to these alleged 'new' challenges,

[8] For instance, a Cisco commissioned value index study [172] placed the value of potential global corporation profits generated by Internet of Things technologies at an estimated $613 billion during the 2013 calendar year.

and are all longstanding concepts that have affected people across both print and digital eras.[9] Furthermore, the digital phenomenon of trust erosion is a problem to address now, let alone within a matured Future Internet environment. However, this is not to say that regulation will not have to adapt and evolve with these wider and ongoing technological, socio-cultural, political, economic and ethical developments. For instance, European policy makers are already shaping the future of data protection law through the proposed General Data Protection Regulation (see Section 4.3.3 for further information).[10]

4.3.2. European legal measures: hard and soft

There are numerous types of legal measures that can be employed through European Union (EU) law. Primary EU legislation refers to the treaties ratified by the member states [15]. Secondary EU legislation encompasses: regulations, directives and decisions [16].[11] Alongside these legally binding measures, the European Commission (EC) can also issue non-legally binding measures: recommendations (e.g. the EC proposes a voluntary action to an institution without legal consequence); and, opinions (e.g. a non-binding statement made by the EC about the practices of a certain institution) [17].

Legally binding measures are often referred to as hard law; whereas, non-legally binding measures are commonly known as soft law.[12] Soft law measures take a variety of forms, including: codes of conduct [18], gentlemen's agreements [18], guidelines [19, p. 754], interpretations [19, p. 754], joint communiqués or declarations [18], notices, guidelines and communications issued by the EC [20, pp. 56-57], resolutions adopted by or within an international organisation [18], and (industry) standards [20, pp. 56-57]. Soft law measures offer pre- and post-legislative advantages. Soft pre-legislative legal measures can provide an anticipatory function by filling legislative gaps where (hard law) regulation is currently uncertain or lacking [21, p. 592]. Soft post-legislative legal measures (e.g. technical standards, guidelines for compliance and organisational procedures) can help to ease uncertainty for stakeholders where hard legislative provisions are ambiguous [22, p. 355].

[9] The often cited and well-known article [182] published by Samuel D. Warren and Louis D. Brandeis discusses privacy and the right to be let alone within the context of 'new' technological advancements in photography and increased media reporting. These privacy concerns raised in 1890 still retain their relevance today.

[10] Furthermore, re-purposing regulatory frameworks for the Future Internet environment has already received attention from legal commentators; especially within the areas of the Internet of Things and cloud computing. For instance, [181] outlines ten actions for the UK Government on how to both maximise the opportunities and reduce the risks of potential Internet of Things technologies – its eighth recommended action [181, p. 10] specifically focuses on regulation and legislation; also see [171], [177] and [180].

[11] The European Commission Website [16] states*: "A regulation is similar to a national law with the difference that it is applicable in all EU countries. [/] Directives set out general rules to be transferred into national law by each country as they deem appropriate. [/] A decision only deals with a particular issue and specifically mentioned persons or organisations."*

[12] The concept of soft law has been predominantly used within public international law and European community law literature [18, p. 268]. However, there is no one definition [18, p. 271], [21, p. 583], [164, p. 70], [165, p. 699]. K.C. Wellens and G.M. Borchardt [18, p. 282] offer a concise definition of soft law: *"[s]oft law involves legally non-binding rules of conduct, not enforceable rights and obligations of public international law."* Furthermore, Fabien Terpan [164, pp. 70-71] highlights: *"[t]hree possible meanings [/] arise from the existing literature: #1 soft law is limited to non-binding norms with legal relevance, #2 soft law is limited to binding norms with a soft dimension, and #3 soft law combines #1 and #2."* Also see [18, p. 269], [164, p. 70] and [166].

Furthermore, soft law can become hard law e.g. privacy-by-design (PbyD) (see section 4.4 for further information).[13]

Soft law measures often arise through industry-led standardisation, regulation and interpretation of hard law instruments (see section 4.3.3). Such soft law measures are often formed by standards bodies rather than through core legislative institutions (e.g. the European Commission). Traditionally, the "Big Three" [23] standards organisations within the ICT sector have been: the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU). However, more soft rule-making bodies continue to materialise [23, p. 3]; a number of which are already operating within the emerging field of the Future Internet environment.[14] For an overview highlighting several of these significant rule-making groups and organisations refer to 'Table One: Soft Rule-Making in the Internet Environment' in the Annex of this report. The recent ISO standard for cloud privacy is now raised as an existing example of a soft law measure that could have a potential role within a trusted Future Internet environment.

4.3.2.1 ISO standard for cloud privacy

On 1 August 2014, the ISO/IEC 27018:2014 standard was published, which provides a code of practice for the protection of personally identifiable information (PII) in public clouds acting as PII processors [24]. It is described by Sophie Curtis [25] as: "the world's first international standard for cloud privacy". The emergence of ISO/IEC 27018:2014 appears to be in direct response [26] to one of the key aims outlined by European Cloud Strategy which was adopted by the European Commission in September 2012 [27].

On 16 February 2015, Microsoft became the first to major cloud services provider to adopt ISO/IEC 27018 [28]. The British Standards Institute (BSI) independently verified that three of its products – Microsoft Azure, Office 365 and Dynamics CRM Online – met the requirements of the ISO/IEC 27018 standard for the protection of personally identifiable information (PII) in the public cloud [28]. On 18 May 2015, another significant cloud services provider – Dropbox – also announced that it was an early adopter of ISO/IEC 27018 [29], as its Dropbox for Business had achieved independent certification through EY CertifyPoint [30]. On a practical level, internationally agreed standards can provide a useful point of reference: "ISO/IEC 27018 also provides a helpful benchmarking tool for legal practitioners engaged in due diligence for new cloud services [31, p. 2]." Furthermore: "ISO 27018 is a great example of a standard 'filling the gaps' between the data protection 'trust' deficit that cloud customers perceive and the highly fragmented, rapidly evolving, unpredictable world of data protection regulation [32]."

[13] Another existing example of this is the draft Microchipping of Dogs (England) Regulations 2015 [173]. These proposed regulations, once enacted, would make it compulsory for all dogs to be microchipped in England. Regulation 4 of the draft Microchipping of Dogs (England) Regulations 2015 states that the microchip used must be compliant with two ISO microchip standards: 11784:1996 [174] and 11785:1996 [175] (apart from Annex A). This proposed hard law instrument therefore contains soft legal measures.

[14] The key advantage of the soft law approach is in its flexibility, as Eilis Ferran and Kern Alexander [19, p. 756] emphasise: "*Soft law bodies are often praised for their flexible decision-making structures. Often comprised of a limited number of participants, they are seen to be able to react quickly to changing circumstances […] These institutional features lead into a further perceived advantage of the soft law concept, namely, that it is a mechanism that can be superior to hard law-making processes in meeting the need for regulation that can be changed and adapted in response to the ever-evolving, highly-complex interactions of the modern world.*"

Despite the potential benefits of ISO/IEC 27018:2014, Mark Webber [33] highlights that it is not an exhaustive framework; and James Mullock [26] states: "[s]igning up this new standard won't provide the silver bullet to all data and cyber compliance issues arising from using cloud based services, but it will offer a credible step in the journey towards compliance and so is a very welcome initiative." As this standard is only partial in the way it regulates the industry, there is a need to adapt a general approach in terms of TWbyD which would be applicable for all types of technologies/scenarios.

In summary, the use of robust soft law instruments should be largely supported, including within a regulatory framework for the Future Internet environment.[15] However, in the context of privacy and data protection, current hard and soft law requirements have been unable thus far to significantly reduce trust erosion. As Inga Kroener and David Wright [34, p. 355] state:

"In recent years, privacy protections have been developed through state regulation or through industry self-regulation. State regulation has been criticized for being underfunded, not enforced, or enforced incorrectly. Industry self-regulation has been criticized for being inadequate for securing privacy."

As a result, there has been a move to further strengthen data protection through a new hard legal instrument – the proposed European General Data Protection Regulation (GDPR) [8] – which is now discussed in section 4.3.3.

4.3.3. European data protection law

4.3.3.1 Directive to Regulation: 1995 to the 2010s

European data protection law is currently governed by the EU Data Protection Directive (95/46/EC) [35], which was enacted in 1995.[16] There are two significant issues with this Directive.[17] First, it is very high level. Different categories of actors are identified, such as data controllers[18] and data processors,[19] but in practice it is difficult to allocate responsibilities. Second, it was not really built to accompany the design and development of new technologies. While it identifies key principles such as data minimisation and data security, it is not clear how these principles need to be implemented in practice.

[15] For information concerning the advantages and weaknesses of self-regulation see [176].

[16] Member states use their own legal instruments to transpose European directives into national law. In the UK, this Directive is implemented through the Data Protection Act (DPA) 1998, which regulates the processing of information which relates to individuals – this includes: obtaining, holding, use or disclosure of such information.

[17] For more information on the strengths and weaknesses of the EU Data Protection Directive (95/46/EC) refer to [205].

[18] The DPA 1998, section 1(1) defines 'data controller': ""*data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed*"". Under section 19 of the DPA 1998, the Information Commissioner must maintain a register of data controllers (subject to organisational exemptions). This Data Protection Public Register [189] contains over 400,000 recorded data controllers (correct August 2015), which is openly accessible on the ICO website and receives daily updates.

[19] The DPA 1998, section 1(1) defines 'data controller': *""data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller".*

In an attempt to overcome this ambiguity and keep pace with technological and societal change, the Information Commissioner's Office (ICO)[20] has published a number of soft law instruments e.g. guidance on "big data and data protection" [36]. However, as previously stated, soft law instruments (such as guidance published by the ICO) have not been enough to foster the development of privacy-sensitive systems alone. Hence there is a pragmatic need to adopt a bottom-up approach that raises legal awareness at the very inception of every ICT project.

At the time this directive entered into force, the World Wide Web was very much in its infancy and there was not the mass utilisation (or availability) of the personal computing devices (such as smart phones, tablets and laptops) that seem to dominant daily-life in 2015. As there has been no major legal upheaval to the European data protection landscape since 1995, it is understandable that the Directive has reached the end of its shelf-life. As Colin Rooney [37, p. 5] expresses: "[t]he EU Data Protection Directive […] has in many regards been found unsatisfactory and out of date, particularly in the age of large scale information processing".

On 25 January 2012, a new draft hard law instrument entered into the fore – the proposed European General Data Protection Regulation (GDPR) [8].[21] Once enacted, the GDPR would repeal the EU Data Protection Directive (95/46/EC), and thus supersede the majority of national data protection laws throughout the European Union [38, p. 175].[22] The definitive version of GDPR is still under discussion;[23] three principle draft versions have been issued by the European Commission [8] on 25 January 2012, the European Parliament [39] on 12 March 2014 and the European Council [40] on 19 December 2014.[24]

At a high-level, the proposed Regulation will provide [41]: (a) one data protection law for one continent; (b) a one-stop-shop for European regulation; and, (c) the same rules for companies processing data obtained from European individuals regardless of which jurisdiction their establishment is based. Bridget Treacy [42, p. 3] highlights: "[t]he proposed regulatory framework is much more detailed and prescriptive than the principles-based regime that we currently enjoy, at least from a UK perspective." In addition to this, Rosario Imperiali [43, p. 285] states that the GDPR "sets forth a new legal regime […] based on a complete compliance program companies

[20] The ICO [188] is the UK's independent authority set up to uphold information rights in the public interest.

[21] In December 2011, a draft of the GDPR proposal was leaked [168, p. 2], [169, p. 12]. On 25 January 2012, the draft was formally published after a two-year data protection review process [168, p. 2], [169, p. 12].

[22] Despite no confirmed date for its resolution, on 12 March 2014 European data protection reform became irreversible following European Parliament vote [197].

[23] The European Parliament, European Council and European Commission were scheduled to enter into trialogue discussions on 24 June 2015 [170]. The GDPR has been the subject of extensive debate and lobbying [44], [169, p. 12], [190]; for critical examination of the proposed Regulation see e.g. [168], [169], [37], [38] and [196]. Some examples of concerns: its potential chilling effect on health sciences research [191]; apprehension over the extent in which the Regulation might constitute an excessive burden to businesses [192]; the controversial higher-rate monetary penalty notices that can be levied on organisation found to be breach of data protection law – up to two percent of global annual turnover [193, p. 6]; how the Regulation is anticipated to apply to companies based outside the EU where they are processing personal data pertaining to EU citizens [41], [194, p. 36]; and how its imposed liabilities in some instances extend to data processors as well as data controllers – this is a potential concern for cloud service providers in circumstances where they qualify as data processors [190].

[24] In July 2015, the European Data Protection Supervisor (EDPS) – Giovanni Buttarelli – launched an EDPS EU data protection mobile app [195], which enables users to compare the latest draft texts of the proposed Regulation.

must demonstrate to fulfil."[25] The GDPR therefore appears to demand a wider cultural shift from the more passive 'hands-off' approach of "**formalistic compliance**" [43, p. 288] (i.e. checking an ICT platform adheres to the prescribed legal minima[26]) to a more active 'hands-on' approach of "**conformity behaviour**" [43, p. 288] (i.e. implementing requirements from the outset of the ICT platform lifecycle that meet the prescribed legal minima and encompass premium options and solutions[27]).

4.3.3.2 Regulation: key considerations

The proposed GDPR – in particular Articles 23 and 33 – has been deliberately chosen as a focal point for Section 4. First, it offers an example of a near 'future legal measure' that, when enacted, is certain to have a fundamental impact on future data processing activities. Especially as the GDPR is set to have a long shelf-life; EU Commissioner Viviane Reding has been quoted [44] stating that: "[t]his regulation needs to stand for 30 years – it needs to be very clear but imprecise enough that changes in the markets or public opinions can be maneuvered in the regulation".

Second, data protection safeguards are crucial for upholding the rights and freedoms of individuals over their personal data. For that reason, the GDPR will be a part of an overall approach to the reduction of trust erosion both now and in the future.[28] Given the high-profile data breaches[29], information asymmetries[30] and advancing technological capabilities of a maturing digital age, it is rather unsurprising that many end-users are increasingly uneasy about their privacy and the security of their personal data.[31] As the digital age matures, a greater number of online ICT platforms generate, process, transmit, store, assimilate and manage increased amounts/types of (non-)personal data from multiple devices and sources [45, p. 396], [46].[32] For instance, an Ofcom

[25] Imperiali [43, p. 287] asserts the proposed GDPR compliance programme is based on the Plan, Do, Check, Act (PDCA) Model Cycle (also known as Deming's Wheel/Cycle). Imperiali [43, p. 287] further states: "*The proposal aims at introducing a legal model in the corporate management structure in order to ensure that personal data are processed in an environment, which provides adequate safeguards. Instead of limiting its intervention to principles and rules of law, the legislator from Brussels has narrowed the entrepreneurial freedom of choice in the management policy, by setting out specific legal provisions and obligations related to corporate organization in order to handle personal data adequately. An overall reading of the document clearly shows the intention of depicting an organic personal data handling system, imposed on data controllers.*"

[26] D2.5: Section 4 authors' interpretation.

[27] D2.5: Section 4 authors' interpretation.

[28] A move towards a Future Internet environment also raises wider ethical questions concerning technological determinism, the over-sharing of personal data and whether current privacy-bargains will be re-drawn for many end users. For more background information about these ethical issues refer to [162] and [163].

[29] Recent high-profile data breaches (in summer 2015) include cyber-attacks on Carphone Warehouse [185] and Ashley Madison [161]. Moreover, passwords have already been stolen from objects as innocuous as smart lightbulbs [160].

[30] I.e. where the provider has better access to information about the collection, management and (re-)usage of an end-user's personal data than the person these data are about. In a number of cases, the absence of transparent processes and policies leaves end-users with a lesser amount of control over their personal data; also see [183].

[31] This uneasiness is highlighted by a recent UK Digital Catapult report [135, p. 8] in July 2015 where: *"60% of those surveyed stated they were uncomfortable sharing personal data [/] 14% admitted they refuse to share any personal data at all [/] 76% of respondents said the main concern in sharing personal data is that they have "no control over how their data is shared or who it is shared with""*

[32] Zhi-Kai Zhang et al. [186, p. 2] illustrate the various types of personal and sensitive data at risk within a Future Internet environment: *"With IoT objects everywhere taking sensitive readings from heartbeats to room temperature at home, it*

report [47], published in May 2014, anticipates that by 2022 over 300 million devices will be connected in the UK alone; machine-to-machine applications are "one of the fasted growing sectors of the wireless communications market" [47, p. 10]. In consequence, if these data protection safeguards are not effectively embedded within Future Internet technologies through both organisational and technical measures; there is potential for privacy and security concerns to depress their uptake [47, p. 18].

Third, the legal obligations imposed on data controllers, such as DPbyD (Article 23) and DPIAs (Article 33), are expected to significantly shape the ways in which certain ICT platforms – those utilised to process personal data – are designed and developed. Mireille Hildebrandt and Laura Tielemans [48, p. 516] state that: "[u]sing technology to implement or enforce legal norms has been coined as techno-regulation."[33] This brings a new dimension to discussions concerning what types of legal measures are likely to have a role in the overall approach to a trusted Future Internet – to what extent should the law assert influence over software engineering in this potential future environment? Should DPbyD provide a specific mandate for technical requirements or impose a new communication strategy [49]?

As a fourth and final reason, Article 23 of the GDPR is an instance where a contemporary of TWbyD (DPbyD is a fellow value-by-design principle) is set to become central to the European legal approach to personal information processing. Therefore, TWbyD has strong resonance with DPbyD as a methodological comparator.

Section 4.4 now raises five key grey areas concerning the implementation of DPbyD as imposed by Article 23 of the GDPR. Through critical cross-comparison, it then evaluates the extent in which TWbyD addresses these five key grey areas highlighted within the proposed legal framework.

4.4. Privacy, data protection and trustworthiness by design

4.4.1. Data protection and privacy: specialised meanings or synonyms?

Article 23 is modelled on the principle of privacy-by-design (PbyD), which was coined, in the 1990s, by Ann Cavoukian – the former Information and Privacy Commissioner of Ontario Canada 1997-2014 [50]. Daniel Le Métayer [51, p. 95] captures the fundamental nature of PbyD in the following statement: "[t]he general philosophy of privacy by design is that privacy should not be treated as an afterthought but rather as a first-class requirement during the design of a system." Jeroen van Rest et al. [52, p. 65] offer an extensive definition of PbyD:

"The principle of 'Privacy by Design' envisions that privacy and data protective measures are operative throughout the entire life cycle of technologies: from the early design stage to their deployment, use and ultimate disposal. This is done by applying a design process that covers all life cycle stages and by applying privacy and data protection design patterns which are well understood and are the known best-practice for the particular purpose they are used for, and domain they are used in. The resulting design documents and systems should limit all the privacy invading activities to the minimum according to the foundational principles of privacy by design."

can be expected that the data in the IoT ecosystem is more personal and dynamic. Because the huge number of IoT devices gather massive sensitive information about users, the data readings about its owner and the personal spaces are treated as personal assets where a leakage may reveal owner's geological location, health status, and living habits. Attackers may extract desired information and disclose personal privacy."

[33] Also see, e.g., [203] and [204] for further information about techno-regulation.

Privacy-by-default is crucial to the successful implementation of PbyD. Privacy-by-default asserts that those directly involved with the design and development of an ICT platform should not regard the inclusion of privacy considerations as a voluntary opt-in or add-on [53]. These two privacy enhancing principles therefore are brought together by Bert-Jaap Koops and Ronald Leenes' [49, p. 159] definition of PbyD: "[p]rivacy by design (PbyD) is the principle or concept according to which privacy should be built into systems from the design stage and should be promoted as a default setting of every ICT system."

However, Article 23 utilises the principles of 'data-protection-by-design' (DPbyD) and 'data-protection-by-default' rather than the long-established concepts of privacy-by-design (PbyD) and privacy-by-default. Privacy and data protection are not identically matched as concepts. Raphaël Gellert and Serge Gutwirth [54, p. 526] distinguish between data protection and privacy by highlighting their differences and where they overlap:

"It [data protection] is narrower because it only deals with the processing of personal data, whereas the scope of privacy is wider. It is broader, however, because it applies to the processing of personal data, even if the latter does not infringe upon privacy. Privacy also is broader and narrower: it might apply to a processing of data which are not personal but nevertheless affects one's privacy, while it will not apply upon a processing of personal data which is not considered to infringe upon one's privacy."

Given that the term privacy is a somewhat vague notion with multiple meanings [55, p. 56], it is rather unsurprising that PbyD has been described as "an amorphous concept" [56, p. 1421] by Ira Rubinstein. Furthermore, Jason I. Hong et al. [57, p. 92] highlight how difficult it is to isolate privacy considerations and its precise applications when the concept of privacy differs between individuals, disciplines and contexts: "[t]he point is that, rather than being a single monolithic concept, privacy is a heterogeneous, fluid, and malleable notion with a range of needs and trust levels."[34] In consequence, Mireille Hildebrandt and Laura Tielemans [58, p. 517] consider the focus on DPbyD to be a "wise decision" as data protection is better-defined than the concept of privacy. However, there has also been criticism that by focusing on DPbyD alone, the GDPR does not go far enough to protect the right to privacy [59]. Furthermore, this shift in terminology may cause potential confusion for those already developing PbyD methodologies. On a practical level, it will be of interest to observe whether stakeholders regard DPbyD as a synonym for PbyD or recognise a "specialization of meaning" [60, p. 260].

This narrow focus on data protection and privacy is also problematic, as PbyD and DPbyD aim only to entrench one value across the entire lifecycle of an ICT platform [61]. This narrow focus therefore overlooks a number of other critical values and issues pertinent to the effective utilisation of ICT platforms, such as intellectual property law issues [62].[35] In contrast, the focus of TWbyD is much

[34] Scott Lederer et al. [156, p. 440] further emphasise how different stakeholders continue to approach the concept of privacy without consensus: *"[r]ather than exposing an unambiguous public representation for all to see and comprehend, it cloaks itself behind an assortment of meanings, presenting different interpretations to different people. When sociologists look at privacy, they see social nuances that engineers overlook. When cryptologists consider privacy, they see technical mechanisms that everyday people ignore. When the European Union looks at privacy, it sees moral expectations that American policymakers do not."*

[35] Alistair Maughan [62] states: *"[c]learly, privacy and data security issues are fundamental to any IoT solution. But it's also important to realise that many IoT solutions do not involve any kind of personal data to which regulations might apply. Data security might still be an issue, but the regulations underpinning the transfer of personal data overseas or securing appropriate consents to data are unlikely to apply. Conversely, issues around ownership of data and IPR are likely to be raised in almost any scenario. It is fundamental to determine whether and how issues of IPR ownership and licence rights are addressed, and whether those rights are wide enough to cover the intended use.*"

wider as, where relevant, trustworthiness subsumes the concepts of privacy and data protection. A sole legal focus on DPbyD further neglects to take forward the wealth of other value-by-design approaches that largely emanate from the human-computer interaction (HCI) domain. This includes: critical design, critical technical practice, ludic design, participatory design, reflection-in-action, reflective design, values at play, value-consciousness design, and value-sensitive design; for further information see [61, p. 26], [63], [64].

4.4.2. Identifying its debtors

In the three draft versions of Article 23 (refer to Table 2 in the Annex) DPbyD is imposed on controllers (the European Parliament version also includes the processor where necessary) and not ICT platform designers and developers. Article 4 of the GDPR defines a controller: "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes*, conditions* and means of the processing of personal data […]". This could be seen as problematic [49, p. 162], [65], [66, p. 51], as this could mean that the obligation is actually imposed too late. Luiz Costa and Yves Poullet [60, p. 260] capture this point in the following question: "[g]iven that the design of technology is essential in this approach why is there no reference to designers?"[36] According to Mireille Hildebrandt and Laura Tielemans [58, p. 517]: "[t]he idea seems to be that by making data controllers responsible (and liable), they will force developers to come up with the right types of technologies." However, controllers may have little or no involvement over the design and development of an ICT platform in practice; e.g. where they are purchasing an off-the-shelf solution, using external cloud services and outsourcing their IT requirements to a third party. Non-compliant ICT platforms may enter the market and the obligation therefore appears to be for the controller to check for DPbyD after design and development phases. However, the onus for DPbyD should not solely lie with software developers and system architects, but other key stakeholders who have direct involvement with and influence over the design and development processes [55, p. 64], [67, p. 23]. Other experts – such as legal professionals, risk managers and data protection officials – are in the best-position to inform this technical implementation by raising pertinent legal, socio-cultural and ethical issues. As Olivia Whitcroft [68, p. 3] states: "during an app's lifecycle, there are many different roles for various parties to play". Article 23 therefore fails to address the technology providers, who do not fall under the category of controllers, and their range of experts who are best-placed to implement DPbyD.

Furthermore, the GDPR advocates the position of the data protection officer (Article 35), but overlooks the role of the privacy engineer. In 2010, Stuart S. Shapiro [69] emphasised the pressing need for privacy engineers to facilitate successful PbyD implementation:

"There's little doubt that appropriately trained engineers (including security engineers) are key to supporting the effective translation of principles, models, and mechanisms into system requirements. There doesn't yet appear to be such a thing as a privacy engineer; given the relative paucity of models and mechanisms, that's not too surprising. Until we build up the latter, we won't have a

[36] Mireille Hildebrandt and Laura Tielemans [58, p. 520] further state: *"[t]he most salient is the question of whether this obligation should not be addressing technology developers directly. To the extent that basic data protection requirements can be articulated at the level of a personal data processing system, irrespective of its further contextualisation, arguments can be given that the compensation objective may be better served if those who fabricate and sell such systems are targeted. A liability similar to product liability could be constructed."*

sufficient basis for the former. For privacy by design to extend beyond a small circle of advocates and experts and become the state of practice, we'll need both."

This leads to a wider concern – whether there is a potential skills shortage in the area of DPbyD, and if so, to what extent this will have an effect on its implementation in the short to medium term?

4.4.3. Identifying the content of the obligation

While DPbyD and data-protection-by-default are welcomed [70], it is difficult to identify the exact content of the obligation; Colette Cuijpers et al. [71, p. 14] state: "[t]he exact meaning of what privacy by default entails is unclear."[37] Ira S. Rubinstein [72, p. 7] further contends: "[t]his new requirement of data protection 'by design and default' is very promising but much depends on how it is implemented."

In all three draft versions of Article 23, identifying the content of the obligation is problematic. There is no clear approach outlined for the implementation of DPbyD; there are vague references to "technical and organisational measures". However, it is unclear what these would encompass. Furthermore, Article 23 appears to be more concerned with the action of processing data rather than the underlying ICT platform employed to carry out this processing. This focus seems to be misplaced, surely the primary concern must be on data protection as – in the words of Daniel Le Métayer – "a first-class requirement during the design of a system" [51, p. 95]. Considering that data processing is reliant on robust technical and organisational data protection safeguards built into ICT platforms, data processing is a secondary concern. It is uncertain whether Article 23 necessitates: (1) mere legal compliance; (2) the imposition of additional organisational measures; and/or (3) the obligation for mandatory technical standards.

First, it is unclear whether Article 23 actually requires more than "mere" compliance with data quality and data security principles.[38] For instance, "[d]ata protection by default is evidently related to the data minimization principle" [60, p. 260]; this is made explicit in the European Council draft text of Article 23. One interpretation is that where processing practices comply with the proposed Regulation, data protection is implemented by default. Further add-ons would be required in the case that processing practices do not comply. Moreover, Luiz Costa and Yves Poullet [60, p. 260] raise another rhetorical question: "[d]oes Data Protection by Design imply embedding in technologies other values than privacy and security?"

Second, it is uncertain whether Article 23 requires the imposition of additional organisational measures. For instance, another way of making sense of data protection by default would be to require proof from the data controller that organisational measures have been put in place at the earliest point in time to make sure privacy risks have been correctly identified and mitigated before the beginning of the processing. While this interpretation is attractive, it is once again arguable that it is imposed too late as it only burdens the data controller and not the technology provider. Moreover, the question arises as to what extent this requirement would differ from the requirement of undertaking a privacy impact assessment which is once again only imposed upon data controllers.

Third, it is ambiguous whether Article 23 requires specific technical measures to be adhered to by data controllers. Mireille Hildebrandt and Laura Tielemans [58, p. 520] state: "[o]ne criticism could

[37] Data protection by default is also described as "unclear" by [157, p. 13].

[38] For more information about the relationship between the concepts of privacy and security see [201].

be that it [Article 23] violates the technology neutrality of the law, by interfering with technology design instead of merely addressing its usage." In response to the apparent techno-legal nature of Article 23, Bert-Jaap Koops and Ronald Leenes [49, p. 168] emphasis the need to focus on changing the mind-set of system designers and developers rather than drafting technical specifications via Article 23(4):

"If privacy by design is to materialise in practice, the European Commission and other regulatory bodies would do well to focus their efforts not so much on attempting to draft further technical specifications […] privacy by design may need to be located no so much in the 'code' section of the regulatory tool-box, but rather in the section containing tools that regulate through 'communication'."

Furthermore, Matthias Pocs [65, p. 649] strongly maintains that a methodological approach to DPbyD must be differentiated from IT security standards. This distinction is drawn because such standards do not address "the promotion of the individual's rights and freedoms" [65, p. 649]. Therefore, Pocs [65, p. 641] further argues that: "Article 23(4) […] does not correctly implement the principle pf PbyD because it lacks a method of legal technology design". Ultimately, according to Pocs, multi-disciplinary engagement (between lawyers and software engineers) is the way forward to defining a robust methodology [65, p. 649]. Luiz Costa and Yves Poullet [60, p. 262] further highlight the importance of an interdisciplinary dialogue within this process:

"In principle, the techno-legal approach (data protection by default, data protection by design) and the duty to initiate a data protection impact assessment are appropriate tools for ensuring the effectiveness of the proposed protection. But at the same time it introduces reliance upon technical expertise to solve societal debates if there is no real debate as regards these technical choices."

In consequence, an overarching grey area is: to what extent techno-legal measures will have a role in the overall approach to a trusted Future Internet (not only within the data protection sphere but) across the entire legal spectrum, and whether this type of approach is justified?

PbyD has also been understood in many different ways; it is therefore unsurprising that there is no common approach to or set of methodologies for its implementation [51, p. 95], [73, p. 39]. An extensive European Union Agency for Network and Information Security (ENISA) report published, on 12 January 2015, by G. Danezis et al. [74] emphasises this point and identifies how PbyD/DPbyD could be implemented through existing methodologies. Refer to 'Table 3' in the Annex for an overview of several significant methodological approaches to PbyD raised by various commentators.

A key difficulty for realising PbyD/DPbyD is translating core values (i.e. its theoretical basis) into counterpart technical requirements (i.e. functional PbyD/DPbyD) and embedding them into the system architecture. Another key difficulty is translating these core values into workable organisational practices. It is a wider cultural change that is required. This is illustrated by: Sarah Spiekermann and Lorrie Faith Cranor [75] who both differentiate and highlight the connection between policy-by-design (i.e. more qualitative approaches) and architecture-by-design processes (i.e. more quantitative approaches); Hoepman [76] who builds on [75]; and Seda Gürses et al. [77] who distinguish between 'hands-off' (i.e. theoretical) and 'hands-on' (i.e. pragmatic) approaches (see 'Table 3' in the Annex for further information). The effective implementation of PbyD/DPbyD requires a blend of both qualitative and quantitative approaches, and this seems to be reflected in all versions of Article 23(1) which refer to "technical and organisational measures". Non-technical guidelines and principles, such as [78] and [79], are required to inform technological implementation of PbyD/DPbyD by outlining core values that need to be considered and incorporated into the system design and development. Reciprocally, technical modelling of PbyD/DPbyD core values, such as [80], is necessitated not only to create privacy-aware systems, but to re-scope the core values in keeping with what is pragmatically feasible.

4.4.4. The impact of cost on implementation

A key barrier to the uptake of PbyD has been the level of cost, time and resources required for its successful implementation [81]. For instance, 4Info – a technology company providing a mobile advertising platform – found that it cost 30% more to store data in a system purpose-built for privacy protection than in a less secure system [81]. Furthermore, the uptake of PbyD has been limited without a legal mandate, as such a strategy is likely to conflict with existing corporate interests [82]. In some cases, customer data may not even form part of an organisation's strategic asset management [73, p. 39]. As Ira Rubinstein [56, p. 1436] highlights, encouraging organisations to change their existing practices is often challenging and complicated due the number of considerations that first must be taken into account:

"In deciding whether to invest in privacy by design, firms engage in a complex cost-benefit trade-off involving the direct, indirect, and opportunity costs of such investments; the effectiveness of various technologies and other privacy safeguards in reducing risks and associated losses; the demand for such technologies and safeguards; the competitive advantage gained by deploying them; and the opportunity costs associated with any technologies that may limit or prevent processing of personal data."

Another important consideration is to what extent the DPbyD approach integrates with or supersedes legacy systems and other related practices. While DPbyD is set to become a legally-binding requirement, Article 23(1) permits the controller to take into account "the cost of implementation" when considering what appropriate technical and organisational measures are required for effective DPbyD implementation. The exact cost threshold is unclear – this leads Luiz Costa and Yves Poullet [60, p. 260] to raise another unanswered question: "[h]ow will the cost of implementation interfere with the responsibility of the controller?" In consequence, Article 23 may not be strong enough to incentivise organisations to fully address the changes required for high quality DPbyD implementation, as they may argue that certain DPbyD features were excluded from the design and development of an ICT platform on cost grounds (or customer requirements grounds).

4.4.5. Evidence-base: accountable DPbyD implementation

From the three draft versions of Article 23, it is clear that controllers must ensure that DPbyD is taken into account before data processing begins. However, as there is currently no set of common methodological approaches to DPbyD, it appears that organisations will select their own (potentially bespoke) method. While greater standardisation is preferable, a tailored approach may be justified as there are many types of personal data each requiring different levels of access and control. For example, personal health care records may require greater forms of protection than a list of customer preferences.

Regulatory authorities do not have the staff and level of resources to check that every ICT system being designed and developed meets the requirements of data protection law (and beyond); they are not "privacy policeman" [83]. In consequence, a data controller's evidence-base for DPbyD implementation will be one of its most important assets. This evidence-base should not only encompasses the system architecture (i.e. proof in design), but a robust audit trail documenting aspects such as the decision-making process, stakeholder engagement, modifications, justified methodological approaches, and applied principles (i.e. proof through provenance). Where possible, it should be open to third party scrutiny to confirm that the ICT platform in question complies with GDPR. A key evidence-base for DPbyD is the data impact assessment (DPIA) approach imposed by Article 33; this is explored in section 4.5.

DPbyD is meant to be a proactive approach to data protection. However, some organisations might not proactively ensure that DPbyD is being implemented correctly. Therefore, rigorous scrutiny of a DPbyD implementation may happen at a much later stage in the ICT platform lifecycle. For instance, if an organisation opts for PbyD transparency, they may choose to have their ICT platform certified by an authoritative third party organisation or publish a report outlining DPbyD implementation. Moreover, for other organisations, their DPbyD implementation is only likely to be called into question in response to an (alleged) data breach where there have been no other robust checks conducted. Does this undermine the accountability and therefore whole purpose of this approach? Although self-evident, for DPbyD to be effective, its implementation must be of high quality and held to account.

The provision of a strong evidence-base is therefore raised as a significant grey area for accountable and transparent DPbyD implementation. While controllers, always, must strive for high quality DPbyD implementation, "perfection" may not be achievable (especially on a first attempt) e.g. due to limited funding, time and resources. This is recognised by Article 23(1) i.e. the controller is able to take into account "the cost of implementation". In consequence, controllers will have to demonstrate why their approach is justified and fit for purpose by capturing their underlying and supporting decision-making processes. This evidence-base will also be able to show areas that can be strengthened and made more efficient within future DPbyD implementations.

4.4.6. Interim evaluation: TWbyD and DPbyD

In summary, while the proposed GDPR Article 23 DPbyD approach is largely welcomed, the following key grey areas are raised with regard to its successful implementation: **(1)** its **focus on data protection** rather than privacy; **(2)** how to **identify the content of the obligation**; **(3)** how to **identify the status of its debtors**; **(4) cost considerations**; and **(5)** its **evidence-base**.

The TWbyD approach largely addresses the key grey areas raised in respect of the Article 23 DPbyD approach. First, OPTET has established a shared terminology in the D2.1 report [2], e.g. definitions of trust and trustworthiness, through interdisciplinary dialogue. Furthermore, it has a wider focus than DPbyD and PbyD. Privacy and data protection are not the only legal areas which impact on trust erosion. Where the purpose and context of a specific ICT platform gives rise to privacy and/or data protection issues, TWbyD may also subsume DPbyD and PbyD principles. Second, OPTET provides well-defined terminology, methodology, tools and guidance for TWbyD, which surpass the current level of detail offered by Article 23. It also considers both the quantitative and qualitative aspects of the value-by-design approach. Third, the TWbyD terminology, methodology, tools and guidance are largely aimed at those at the coalface of ICT platform design and development – the system designers and developers. Furthermore, OPTET has conducted stakeholder analysis to consider the key roles involved with the entire lifecycle of an ICT platform. It is explicitly recognised there is both an intellectual and pragmatic need for interdisciplinarity to both shape and apply a TWbyD approach. Fourth, OPTET has openly released a significant amount of information pertaining to the TWbyD approach. Therefore, it is hoped that this will help to reduce costs and resource burdens for organisations as they will be able to re-use and build on these evidence-based trustworthiness management methodologies and technologies – there is no need to "reinvent the wheel".

In consequence, while Article 23 is largely welcomed, it needs to address the key grey areas outlined. The TWbyD approach offers a good case in point for strengthening DPbyD; in particular its focus on interdisciplinarity that has facilitated a shared terminology, methodology and tools. Section 4.5 now focuses on the, arguably, most significant final grey area – the provision of a strong evidence-base for accountable and transparent Article 23 compliance – by focusing on three significant models of legal awareness and laying the foundations for the OPTET Legal Integration Model (OPTET-LIM).

4.5. Evidence-base for value-by-design: legal awareness models

Key stakeholders involved with the design, development and deployment of ICT platforms need to conduct organisational-level (and where possible independent third party) evaluation. This scrutiny is required to ensure and demonstrate that a particular asset (e.g. a trustworthiness application), at the bare minimum, complies with legal obligations. This section explores three key legal awareness models that can be used to verify the extent in which: a value-by-design approach (e.g. TWbyD, DPbyD and PbyD) has been successfully implemented; and, that the resulting ICT platform conforms to minimum legal standards and other optional premium criteria. These three legal awareness models are: (1) legal compliance checks, (2) Article 33 of the GDPR – data protection impact assessments (DPIAs), and (3) Article 39 of the GDPR – certification and seals. This section then draws attention to the distinction between legal awareness and the pragmatic need for wider legal integration through OPTET-LIM.

4.5.1. Legal compliance checks

Legal compliance checks[39] are widely used as a method to: (a) confirm that an ICT platform conforms to minimum legal requirements; and (b) identify any further measures, if necessary, to avoid non-compliance [83].[40] Legal compliance checks were not originally designed to co-ordinate with a value-by-design approach. Therefore, this legal compliance check will usually occur once during the latter stages of system development or when an ICT platform is operational [59, p. 127]. This method is therefore described as "**intrinsically reactive**" [84, p. 667], as any changes required as an afterthought are usually costly [59, p. 127], [85, p. 8]. Moreover, these legal compliance checks generally take the form of a tick-box exercise, which are often carried out by non-technical experts (e.g. legal professionals and data protection officials) without or with limited consultation of system designers and developers [59, p. 127]. Furthermore, there is a lack of standardisation [59, p. 127]; therefore, each organisation is likely to have its own procedures.

4.5.1.1 Interim evaluation: legal compliance checks

In summary, the legal compliance check approach to legal assessment appears to suffer from five fundamental weaknesses: **(1)** its **narrow focus on compliance** without inclusion of other premium options; **(2)** its **responsive** rather than proactive nature; **(3)** its **solitary 'snap-shot'** method; **(4)** its **tick-box format**; and, **(5)** its **lack of/limited interdisciplinary dialogue**.

[39] Also known as legal compliance audit or legal compliance analysis.

[40] A controller may also undertake separate IT security checks [85, p. 8].

4.5.2. Privacy/data protection impact assessments

In 2007, the Information Commissioner's Office (ICO) in the UK became the first European regulator to publish privacy impact assessment (PIA) guidance [86], [87, p. 55], [88, p. 2].[41] The ICO PIA Code of Practice offers a "broad and flexible" [86, p. 5] definition of a PIA:[42]

"Privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved."

Monica Salgado [89, p. 3] further contends that: "PIAs are, essentially, due diligence exercises aiming at assessing the impact that new technologies or projects will have on individuals' privacy rights." PIAs are also a form of legal risk assessment, as Luiz Costa [90, p. 18] states:

"Risk assessment is a procedure by which one distinguishes non-plausible from plausible risks and graduates the possibility of the last ones to occur. PIA is a sort of risk assessment since it aims to evaluate the potential consequences of an activity on privacy and data protection."

Privacy impact assessments have a pivotal role in a PbyD approach [91, p. 13], [86, p. 4], [92, p. 8], as Inga Kroener and David Wright [34, p. 360] state:[43]

"In our view, PbyD is more than a set of principles: It is also a process, which is intimately tied to the design process. For process guidelines, we invoke the privacy impact assessment process. A privacy impact assessment can help identify privacy risks. Identification of risks can spotlight areas where PbyD principles can be employed to develop effective solutions."

While privacy impact assessments (PIAs) and data protection impact assessments (DPIAs) are currently without legal status, under Article 33 of the proposed GDPR, DPIAs would become a legal requirement.[44] David Wright et al. [93, p. 163] state: "[a] PIA should: [/] Be more than a compliance check; [/] Be a process; [/] Be reviewed, updated and on-going throughout the life a project." In general terms, PIAs and DPIAs are employed as a method to: (a) confirm that an ICT platform conforms to minimum legal requirements; (b) identify any further measures, if necessary, to avoid non-compliance; and (c) determine "optimum privacy options and solutions" [83] which go beyond the legal minima. This latter category (c) broadens the scope of legal assessment further than a mere legal compliance check [87, p. 55], [90, p. 19], [94, p. 292], [91, p. 13]. Furthermore, a PIA

[41] The most recent version of this guidance – Conducting Privacy Impact Assessments: Code of Practice – was published in 2014 [86]. This guidance was the result of an ICO commissioned team of experts from Australia, Canada and the UK, led by Loughborough University [202, p. 234], which reviewed PIA models in Australia, Canada, Hong Kong, New Zealand and the USA [202, p. 235].

[42] A European Commission Staff Working paper [96, p. i] offers a similar definition of a data protection impact assessment (DPIA): "*[a] process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions."*

[43] For more information about PIAs in practice see: the Privacy Impact Assessment Framework (PIAF) project [218]; and, the European Commission report on Privacy and Data Protection Impact Assessment Framework for RFID Applications [219].

[44] Impact assessments are not only used with the context of privacy and data protection e.g. environmental impact assessments [217].

should occur across the lifecycle of an ICT platform (from cradle-to-grave/cradle) as a continuous inspection mechanism [59, p. 128]. This method is therefore described as "**proactive**" [84, p. 667], as this on-going legal scrutiny is able to inform design and development decisions from the outset [59, p. 128]. As a result "reducing the risk that costly retrofitting of privacy safeguards will be required after implementation" [84, p. 667]. Moreover, PIAs can build on established standardised risk management approaches in order to evaluate and mitigate risks [59, p. 128]; the PIA method surpasses a mere tick-box exercise [94, p. 292], [91, p. 13].[45] A PIA will involve a wide-range of multi-disciplinary experts, e.g. technical and legal professionals [59, p. 128], to ensure legal issues are addressed through required interdisciplinary knowledge bases.

David Wright [87, pp. 55-56] highlights six key benefits of PIAs (refer to article for full explanation): (1) they offer an early warning system; (2) they provide a compliance check and audit trail; (3) they enhance informed decision-making processes; (4) they promote transparency; (5) they are an educational tool for employees; and, (6) they demonstrate to the public and regulators that the business prioritises privacy and takes such matters seriously. Moreover, regulatory authorities can use PIAs as part of an evidential basis for legal compliance and PbyD [83]. David Tancock et al. [84, p. 667] further add:

"Privacy rights are protected and advanced by convincing agencies and businesses to carry out a PIA for the following reasons: to demonstrate legal compliance, to allow organisations to develop better policies, to save money, to develop a culture of privacy protection, to prevent adverse publicity, and to mitigate risks in advance of resource allocation."

While in theory, PIAs and DPIAs are a more advantageous approach to legal assessment than sole reliance on the legal compliance check approach, the ways in which Article 33 has been drafted has raised a number of grey areas for concern amongst commentators.[46] Sub-sections 4.5.2.1-4.5.2.5 will now explore these grey areas.

4.5.2.1 Article 33: its focus

The focus of Article 33 is on **data protection** rather than privacy. As previously stated, data protection and privacy are not synonyms [54, p. 526]. The GDPR again departs from the terminology – "PIA" – commonly used throughout the literature and by regulatory authorities (such as the ICO). Therefore, as with DPbyD and PbyD, once more there is difference of opinion on the varying scope of PIAs and DPIAs.[47] Moreover, a focus on data protection and/or privacy alone, when evaluating

[45] Stephanie Pritchett [91, p. 13] states: *"[t]he introduction of mandatory DPIAs will force organisations to carry out a greater level of data protection due diligence before undertaking riskier data processing activities. Crucially, this work will only be effective if organisations carry out reasonable risk analysis assessments to ensure 'privacy by design' and where meaningful reports are produced, as opposed to organisations simply completing a bureaucratic box ticking exercise (or sub-contracting this work to data processors without proper consideration)."* David Wright and Charles Raab [94, p. 292] further contend: "*[d]ecision-makers would do well to avoid a strictly compliance-based approach to privacy risk. At a time when privacy appears to be threatened more than ever before, and by novel kinds of surveillance, further guidance could be given to industry and others to uncover privacy risks by using sets of questions to identify privacy risks, rather than ticking some boxes on a form."*

[46] One notable contribution is a comparative analysis of six jurisdictional approaches to PIAs (within Australia, Canada, Ireland, New Zealand, UK and USA) conducted by David Wright et al. [93], which identifies the key best practice elements absent from Article 33.

[47] For instance, David Wright et al. [93, p. 163] prefer the term PIA over DPIA because: *"[t]he former is wider-ranging and can catch intrusions and compromises that may not be caught by a data protection impact assessment."*

the lawfulness of a data processing activity, is a potential drawback in itself. PIAs and DPIAs scope is likely to be narrower than a more general legal compliance check, which takes into account a wider-range of legal areas e.g. competition law, contract law, information security law and intellectual property law.[48]

Licensing scenario
A controller wants to create a new ICT platform capable of processing thousands of personal records from multiple sources. In accordance with the GDPR, the controller ensures that from the outset the new ICT platform is designed and developed in accordance with Articles 23 and 33. However, while the controller meets data protection requirements, (s)he has failed to consider the licensing risks associated with processing data from multiple sources; the personal records are sent to the controller under an assortment of licence agreements (including various attribution statements). The controller therefore realises that (s)he does not have the authorisation to carry out certain processing activities, and is in breach of a number of licensing agreements.

In consequence, controllers (and potentially processors) need to be aware that data protection law is only one legal obligation amongst many. However, PIAs/DPIAs may have a secondary effect where there is strong interdisciplinary dialogue. Legal experts (with a broad knowledge) might also be able to pinpoint other legal areas for concern and compliance issues outside the original focus on data protection/privacy. However, to re-iterate, this very much depends on whether the interdisciplinary dialogue is robust enough.

DPIAs are not an absolute requirement under Article 33(1), a controller will decide whether to undertake one based on an evaluation of the "(specific risks) to/the impact of the envisaged processing operations on/high risk for **the rights and freedoms of data subjects/individuals**". Therefore, a controller may erroneously decide not to carry out a DPIA even though the data processing is a risky activity.

Furthermore, there are questions about the meaning of the "rights and freedoms of data subjects"; Costa and Poullet [60, p. 260] ask the following rhetorical questions: "[w]hat balance will Data Protection Impact Assessment achieve with regard to "rights and freedoms of data subjects"? Is Data Protection Impact Assessment a parameter of a general duty of care? If yes, how will this determine responsibility and liability of actions according to this parameter?" In consequence, how these rights and freedoms are to be interpreted is yet to be determined. Will Article 33(1) extend 'the rights and freedoms' to include privacy? As a final point, Article 33 only focuses on outlining risks and not the particular benefits of the DPbyD approach [93, p. 176].

4.5.2.2 Article 33: emphasis on the DPIA report

The DPIA requirements, imposed by Article 33(1), have been referred to as "**rather sketchy**" by David Wright [95, p. 307] and "**relatively vague**" by Stephanie Pritchett [91, p. 11]. Refer to 'Table Five' in the Annex for an overview of several significant methodological approaches to PIAs raised by various commentators. Given that PIAs and DPIAs are recognised as a process, it seems slightly incongruous that the focal point of Article 33 is on the DPIA report (i.e. the outcome of the process) rather than the process criteria [93, p. 173]. For instance, there is no mention of recording the persons who undertook the DPIA e.g. authoritative contacts for help and advice [93, p. 175]. Moreover, there is no reference to the skill sets required to undertake an effective DPIA e.g. software

[48] Previous work conducted by iLaws in the OPTET D2.1 Report [2, pp. 144-167] has already highlighted a number of significant legal measures not just within data protection law, but contract law and information security law.

engineers, legal professionals and commercial officers [93, p. 175], or the provision of guidance and resources [93, p. 175]. Conceivably this procedural ambiguity could be rectified by separate codes of practice to follow; Article 33(7) reserves the right for the European Commission to "specify standards and procedures for carrying out and verifying and auditing the assessment" [European Commission draft text]. However, this is not guaranteed, and if it does follow, it would leave those undertaking DPIAs in a state of uncertainty during the interim period.

4.5.2.3 Article 33: cost and potential burden to SMEs

According to a European Commission Staff Working Paper [96, p. 69], the cost of a DPIA will vary according to the circumstances of a particular case: "[i]t is estimated that a small-scale DPIA would cost €14,000, a medium-scale DPIA would cost €34,500, and a large-scale DPIA would cost €149,000." While the DPIA approach is largely welcomed, a number of organisations – particularly SMEs – have raised concerns over the potential costs involved with obligatory DPIAs for high risk personal data processing [97, p. 141], [96, p. 81], [88]. Paul De Hert and Vagelis Papakonstantinou [97, p. 141] summarise this uneasiness: "the draft Regulation's approach seems to be insensitive to financial constraints: potentially risky personal data processing is often undertaken by small corporations that may not have the financial means to conduct a proper DPIA."

4.5.2.4 Article 33: on-going interdisciplinary dialogue

Consultation with both internal and external stakeholders is a crucial aspect of the PIA and DPIA process; and is advised by the ICO PIA Code of Practice [86, p. 11]. However, Article 33(4) of the GDPR only gives explicit emphasis to consultation with external data subjects; it states: "[t]he controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations." Furthermore, Article 33 focuses on the controller, and in some cases the processor and data protection officer, as responsible for carrying out a DPIA where necessary. There is no reference given to the software developers and designers, risk managers, legal experts, commercial and other compliance officers required to successfully undertake a DPIA. Therefore, Article 33 alone does not guarantee the necessary level of on-going interdisciplinary dialogue necessitated for a robust DPIA. Once again, Article 33(7) reserves the right for the European Commission to specify further standards and procedures; however whether future codes of practice will cover enriched consultation and improved interdisciplinary dialogue is yet to be determined.

4.5.2.5 Article 33: accountability

Kroener and Wright [95, pp. 313-314], [34, p. 362] both contend that for the DPIA approach to be effective it requires "teeth" i.e. a robust mechanism for accountability – a feature which it is currently lacking. As far as is possible, any legal assessment must be transparent and open to third party scrutiny. This is to ensure that the legal assessment carried out is both reliable and fit for purpose. However, Article 33 does not directly impose any form of independent scrutiny on DPIAs either externally or internally. In contrast to the ICO PIA Code of Practice [86], Article 33 makes no reference to the open release of (redacted) DPIA reports for public scrutiny [93, p. 175]. Instead, effective DPbyD and DPIA implementation appears to rely on an expectation of goodwill and trust on the part of the controller (and potentially the processor) alone [97, p. 141]. To rectify this lack of accountability, DPIA reports should be openly released where possible [93, p. 175], a DPIA registry [93, p. 175] could be set up as a record of DPIA implementation and copies of DPIA carried out by public bodies could be sent to the regulatory authority to be safeguarded for future use (if required) [93, p. 176]. Moreover, Article 33 could be expanded to preserve the right for privacy commissioners to review and provide guidance on DPIA reports where necessary [93, p. 176].

While it is not possible to a have a system without human error or malpractice, the DPIA approach could be subject to (un)intentional misuse. For instance, a controller could fraudulently claim that a DPIA took place but the report has subsequently been lost or deleted. If a DPIA report was requested in light of an alleged data protection breach, a DPIA report could be falsified or copied. A controller could undertake a review, but its quality could be sub-standard. Moreover, a controller could wrongly choose not to undertake a review, as carrying out a DPIA is not an absolute requirement under the GDPR. Therefore, should some form of legal assessment be made mandatory under all circumstances e.g. legal compliance checks?

Yet again, as Article 33(7) reserves the right for the European Commission to specify standards and procedures, perhaps these will focus on making the DPIA approach more accountable and independent. To resolve this issue an obligation to disclose could be introduced i.e. the final DPIA report must be openly released (where possible and potentially in a redacted form) on the controller's website. The ICO Code of Practice for PIAs already advises this disclosure.

4.5.2.6 Interim evaluation: Article 33 DPIA approach

In contrast to the legal compliance check model, the proposed GDPR Article 33 DPIA approach has been purposefully-designed to complement DPbyD implementation. Therefore, the proposed GDPR Article 33 DPIA approach to legal assessment overcomes the majority of weaknesses found within the legal compliance check model: (i) it focuses on both compliance and premium options; (ii) it is proactive; (iii) it is a process that spans the data processing lifecycle (i.e. from cradle-to-grave/cradle); and, (iv) it goes further than a tick-box exercise.

However, the two key grey areas facing the implementation of the proposed GDPR Article 33 DPIA approach are: (1) its perceived inability to guarantee a sustainable and on-going interdisciplinary dialogue; and (2) its lack of accountability.

4.5.3. Certification and seals: cues for data subjects

The majority of end users are unable to directly verify the trustworthiness attributes of a specific ICT platform. In many instances, privacy and security concerns are exacerbated where there is a lack of information given about how end users' data are stored, handled, used and re-used in both foreseen and unforeseen forms and the lifetime of this information.[49] In order to reduce this information asymmetry between ICT providers and end users (particularly where end users do not have extensive technical knowledge and/or access to underlying technologies), providers can use a selection of signalling methods to better-communicate underlying trustworthiness attributes to end users. One such method is the utilisation of trust marks;[50] defined by this report as:

A trust mark is a symbol used to represent that a website, system, application and/or service has passed a particular set of best practice criteria e.g. for quality, privacy or security. Trust marks are also known by (but not limited to) the following terms: certification marks, authentication marks, quality assurance labels and seals of approval.

[49] OPTET Report D2.4 focused on individuals' responses to legal information and guarantees i.e. signalling (un)trustworthiness through legal signposting/cues.

[50] Another example is the privacy policy. For an extensive overview concerning the role of trust marks and trust mark organisations in e-commerce refer to [209].

In theory, ICT trust marks provide an informative and reliable visual reference point for conveying quality and provenance information.[51]

There are a number of trust mark and certification programmes available for ICT platforms e.g. TRUSTe (USA) and Privacy Mark (Japan) [98]. While, in the past, trust marks for ICT platforms have been more prevalent within North America and Japan, they are receiving greater attention from Europe [98]. Moreover, EuroPriSe and EMOTA are two European organisations already providing trust marks for ICT platforms. EuroPriSe [99] is the European privacy seal for IT products and IT based services; enabling companies to display their privacy compliance.[52] More recently, on 1 July 2015, the European eCommerce Association (EMOTA) launched a European trust mark for online shopping [100], known as: the EMOTA Trust Mark.[53]

Article 39 of the GDPR, actively supports the use of certification mechanisms and seals: "[t]he Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors." While this type of certification offers a very useful mechanism for (independent third party) evaluation and signposting legal compliance and other premium features to end users, it is a largely reactive approach as it usually takes place just before/after ICT platform deployment. Furthermore, certification processes are not all robust (e.g. some mechanisms allow for self-certification which may limit accountability), can be narrow in scope (e.g. only focus on data quality requirements) and in some cases are too common (e.g. it becomes hard to distinguish the differences between ICT platforms if the majority were to be awarded very similar data protection seals).

4.5.3.1 The End to End Trustworthiness Evaluation tool (e2eTWE): cues for developers

Different types of certification can occur within the various phases of an ICT platform lifecycle. As part of the OPTET TWbyD approach, WP3 developed the End to End Trustworthiness Evaluation tool (e2eTWE).[54] The e2eTWE uses certificates of existing software modules to influence the design and development of new software modules or the configuration/deployment of composite ICT systems. This tool enables system designers (as part of a TWbyD approach) to proactively use both legal compliance checks and certificates during the design phase.

[51] Trust marks are used by a multitude of industries. One longstanding example is the familiar hallmark, which are found on items of jewellery to signal the quality and fineness of the precious metal(s) present (as well as other features) [210]. Assaying and hallmarking dates back to the 1300s – and is described as *"one of the oldest forms of consumer protection that exists"* [210]. Another enduring example is the 'BSI Kitemark', an internationally renowned conformity certification trade mark, which originated in 1903 as the British Standards Mark for use on tramway rails [211]. It is owned and operated by the British Standards Institute (BSI) and now covers a range of products and consumer services [211]. Eco-labels are another type of trust mark; refer to the Ecolabel Index [212] – a global directory tracking over 450 ecolabels. For further information concerning the legal and commercial issues surrounding ecolabels see [213].

[52] For further background information see [208] . Furthermore, on 13 July 2008, Ixquick – a meta-search engine based in the Netherlands – became the first recipient of the EuroPriSe privacy seal [206]. According to EuropPriSe's Register of Awarded Seals, there are currently twenty active privacy seals [207] (correct on 19 August 2015).

[53] Its release was welcomed by the European Commission as a means to facilitate and increase online purchasing across member states: "[t]oday's launch will help build consumers' trust in the digital world. Currently, only 15% of European consumers buy online from other Member States" [100].

[54] See OPTET D3.4 Report [228] for full information.

Given that Article 39 of the GDPR only focuses on signalling data protection information to data subjects (through data protection seals), it appears to provide a limited approach to certification. For instance, unlike TWbyD, it does not take into account how certification can also allow system developers (and other interested parties) quick access to the level of data protection and/or trustworthiness offered by a particular software module. In consequence, a careful distinction needs to be drawn between those certification mechanisms which are primarily aimed at: (a) data subjects (i.e. end users) which are largely reactive e.g. Article 39; and, (b) system designers which may have a proactive function e.g. e2eTWE.

4.5.3.2 Interim evaluation: certification and seals – cues for data subjects

Similar to the legal compliance check model, certification and seals that are used as cues for data subjects are not designed to be implemented from the preliminary stages of ICT platform design and development. Therefore, if an ICT platform failed to pass certification, any required changes may be costly and disruptive. However, this type of certification is a very valuable mechanism and should be welcomed as part of the GDPR.

4.5.4. Interim evaluation: TWbyD and legal awareness models

Despite a number of a key grey areas, it is clear from the examination of the three legal awareness models that the DPIA approach provides the most robust evidence-base for value-by-design. However, the TWbyD evidence-base goes further, as is now explained.

(a) In what way does TWbyD go beyond the Article 33 DPIA approach?

In contrast to DPbyD, the focus of TWbyD is not restricted to data processing. TWbyD applies to any ICT platform regardless of the level of associated risk or whether any data protection (and/or privacy) issues subsist. For instance, it may potentially subsume issues relating to, e.g., competition law, contract law, information security law and intellectual property law. In consequence, TWbyD has a much wider remit and the potential to apply to situations that fall outside the scope of DPbyD (or PbyD). For instance, the following two scenarios have the potential to fall within the range of TWbyD but not DPbyD and/or DPIA: (a) an ICT platform processing non-personal data from third parties will fall outside the reach of Article 23; and (b) an ICT platform carrying out low risk personal data processing may be subject to Article 23 but not meet the threshold for an Article 33 DPIA.

In contrast to the "rather sketchy" [95, p. 307] requirements imposed by Article 33, OPTET provide a number of robust methodologies, practices and tools to help system designers and developers to effectively implement TWbyD. See WP3 deliverables OPTET Reports D3.1 [6] and D3.2 [101] for more information. TWbyD is not focused on the content of a single report, but specifying the trustworthiness requirements as a process: "capability patterns that "enrich" the standard software development activities" [101, p. 17].

In summary, TWbyD surpasses the Article 33 DPIA approach through its: (1) wider remit, (2) systematic and detailed approach, (3) transparency, (4) accountability and (5) interdisciplinarity. Its approach to the latter two categories will now be explored in depth.

(b) How does TWbyD address the two main (interrelated) concerns – **accountability and interdisciplinarity** – raised by Article 33 of the GDPR?

First, accountability is a core component of the TWbyD approach. Information about TWbyD methodologies, practices and tools are published as part of an extensive series of open access reports available on the OPTET website, which are therefore open to public scrutiny. While self-evident, value-by-design is only as effective as those individuals undertaking them. Furthermore, providing evidence-based compliance is a crucial aspect of the TWbyD approach. Individuals and organisations implementing TWbyD will be encouraged to openly release a list of threats and controls applied,[55] metrics utilised,[56] and a Digital Trustworthiness Certification (DTwC).[57] In particular, the DTwC will act as a signpost to third parties to show that an ICT platform has met certain trustworthiness criteria.

Second, as TWbyD has been designed by an interdisciplinary team composed of computer scientists, economists, social scientists and legal experts, interdisciplinarity is at the very heart of this approach. Furthermore, there has been extensive stakeholder analysis throughout the research packages. For instance, the OPTET D3.2 Report goes beyond the high level roles of system developers and designers by outlining specific positions and skill sets e.g. risk analyser, system trust and trustworthiness architect, system trustworthiness monitor, and system trustworthiness certificate architect. One further example are the use cases undertaken by the OPTET WP8 team.

Despite a fundamental need for a sustainable and on-going interdisciplinary dialogue, this is does not currently seem to be guaranteed within the proposed GDPR; and, it does not form part of the legal compliance check or certification approaches. Article 33 focuses on the controller, and in some cases the processor and data protection officer, as responsible for carrying out a DPIA where necessary. There is no mention of the software developers and designers, risk managers, legal experts, commercial and other compliance officers required to successfully implement and evaluate the DPbyD approach. Furthermore, it appears there is an assumption that the persons responsible for DPbyD implementation and evaluation have the requisite knowledge and access to adequate levels of guidance and support; regrettably this is not always the case.

4.5.4.1 The need for improved legal integration

While it is self-evident, the implementation of a value-by-design approach is ineffective without the necessary interdisciplinary knowledge bases and skilled experts to implement it (e.g. privacy engineers [69]). Bert-Jaap Koops and Ronald Leenes [49, p. 168] emphasise the need to for EU law to regulate DPbyD/PbyD through instruments that promote communication rather than technical specifications (i.e. techno-regulation). In addition, Rosario Imperiali [43, p. 288] appears to view DPbyD as requiring a wider cultural shift from "formalistic compliance" to "conformity behaviour", which is also achieved through improved communication (e.g. "accurate reports and information flows") and understanding (e.g. "compliance training"). Furthermore, Monica Salgado [89, pp. 4-5] highlights the importance of legal awareness amongst key stakeholders: "[i]t is counterproductive to attempt to implement appropriate PIA and PbyD processes when the relevant teams are not data protection aware, and cannot for example identify what constitutes personal data and what constitutes a processing activity."

A sufficient level of legal awareness amongst key stakeholders is required: (a) to successfully implement a value-by-design approach; and (b) for robust evaluation. There seems to be an underlying assumption that all key stakeholders possess a sufficient level of (access to) legal

[55] See WP2 documentation for full information.

[56] See WP3 documentation for full information.

[57] See WP4 documentation for full information.

knowledge to implement GDPR obligations; however this is not always the case. There needs to be greater integration of legal knowledge bases; legal integration is defined by this report:

Legal integration: a state of being well-informed about the status, substance and implementation of pertinent soft and hard legal measures (in force and/or pending enactment) throughout the ICT platform lifecycle. It is built on robust: (1) interdisciplinary dialogue which involves (a) good communication and (b) sufficient legal understanding; and, (2) audit trail.

Improved legal integration is therefore a priority for the design, development and deployment of robust ICT platforms. It should be entrenched into the organisational strategy as an explicit organisational practice. In consequence, the OPTET Legal Integration Model (OPTET-LIM) proposes a holistic, high-level approach to improved legal integration throughout the "Trustworthy Application Cycle" which is now outlined in section 4.6.

4.6. The OPTET Legal Integration Model (OPTET-LIM)

4.6.1. Key legal integration requirements

The OPTET-LIM is composed of two parts: (A) an on-going interdisciplinary dialogue facilitated by (1) an improved legal literacy and (2) access to accurate, timely and reliable legal information; and, (B) a robust audit built on effective (3) legal impact assessment and (4) the disclosure/signposting of legal compliancy and premium trustworthiness features.

4.6.1.1 Part A: on-going interdisciplinary dialogue

Given that legal experts usually are involved in the later stages of software development (such as before product release), there is often a lack of guidance and legal input during initial phases of ICT platform design and development [102].[58] This position needs to be changed. Legal experts should have the opportunity for greater engagement across the ICT platform lifecycle; and non-legal experts require access to support and guidance. The following two requirements – improved legal literacy and access to accurate, timely and reliable legal information – are needed to strengthen legal awareness.

(1) Raise legal literacy

As legal departments (alongside other compliance officers) are largely responsible for due diligence and providing legal guidance, it is unsurprising that there is often a more limited knowledge of legal issues amongst software engineers [74, p. 50], [82].[59] This situation needs to be changed; system designers and developers need greater access to legal expertise and high quality legal information (possibly via creating multi-disciplinary teams). Increased opportunities for e-learning, skills

[58] For instance, Giulio Coraggio [102] states: *"[w]e are working on very interesting Internet of Things projects and the feeling is always that lawyers are involved at the very late stage when the product is already completed and ready to be launched in the very next days. At that stage a "negotiation" between the legal team and the technical and commercial teams starts on what changes can be implemented without requiring further developments/costs, what risks should be taken, and whenever lawyers raise an issue, the technical and commercial teams have almost a "heart attack"…"*

[59] As George Danezis et al. [74, p. 50] state: *"[t]here is a deficiency in awareness and knowledge among system developers and service providers. Traditional and widespread engineering approaches simply ignore privacy and data protection features when realising the desired functionality. The situation is further aggravated by a deficit of current developer tools and frameworks, which make it easy to build non-compliant systems, but nearly impossible to build a compliant one."*

development, training and workshops directly related to legal issues within ICT design, development and deployment are required. Individuals and organisations should also make the most of openly released legal literacy tools from reliable sources. For instance, open access soft law instruments – such as guidelines and codes of best practice provided by authoritative sources (e.g. the ICO, government bodies, research groups and law firms) – are invaluable as a secondary source to raise legal literacy. Furthermore, organisations should take advantage of relevant massive open online courses (MOOCs), where they exist, to further legal understanding. Also, keeping up-to-date with recent legal developments through online media reports i.e. periodicals and social media channels is also useful. Legal literacy cannot be condensed into an annual one-day workshop. Daily business priorities and time may eventually erode legal knowledge. For legal awareness to be sustainable, legal literacy must be an on-going process (or relatively affordable consultancy).

(2) Access to accurate, timely and reliable legal information

Section 4.3 illustrated the complexities with identifying pertinent hard and soft legal measures which apply to the design and development of a particular ICT platform. There may be a manner of cross-jurisdictional issues to contemplate [103, p. 58], various areas of law that apply (e.g. data protection law, contract law and intellectual property law), and a wealth of industry standards to take into consideration. Moreover, key stakeholders must keep up-to-date with legal amendments, repeals, proposals, enactments and case law (at national, European and international levels). Any (automated) legal risk management model needs to be kept up-to-date. Organisations need to consider where to source reliable, timely and high quality legal information. Where an organisation is fortunate to have an in-house legal team, these individuals will constitute the first point of contact for accurate, timely and reliable legal information. Although not a substitute for this professional legal guidance, open access soft law and education programmes from authoritative sources can again provide an up-to-date secondary source of information. Furthermore, organisations might consider offering an internship programme, sponsoring research degrees and post-docs or inviting expert speakers to explore significant legal issues facing the organisation.

4.6.1.2 Part B: robust audit trail

A robust audit trail is required to capture all key qualitative and quantitative elements of a TWbyD implementation, such as its origins, justifications, applied processes and informed decision making throughout the lifecycle of an ICT platform, therefore, strengthening the evidence-base for effective TWbyD implementation. Where possible, these records should be reproducible for external stakeholders, e.g. regulatory authorities, who may later call into question the extent in which TWbyD has been effective in a particular ICT platform. This should be distinguished from a (DPIA) report where the underlying and supporting data may be condensed into a shorter, human-readable summary. This audit trail is strengthened by the following requirements: legal impact assessment, and disclosing and signposting legal compliancy and premium trustworthiness features.

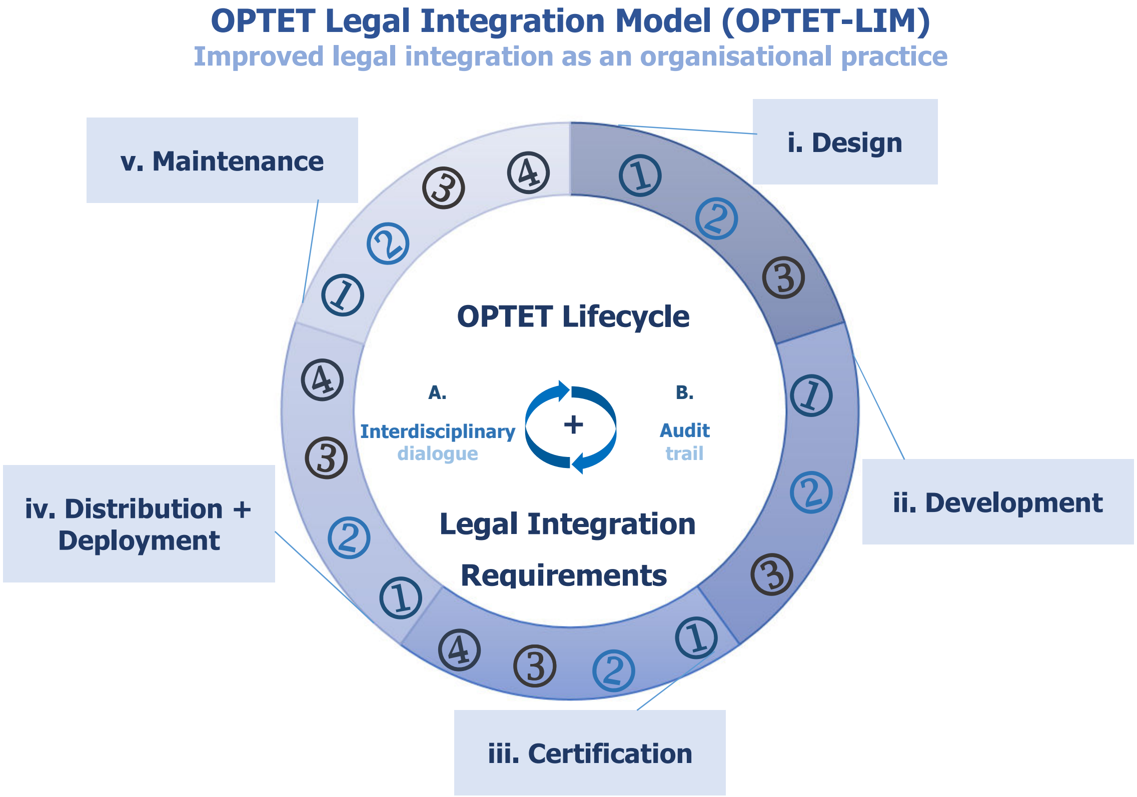
(3) Legal impact assessment

Organisations need to: (1) verify that the specific application conforms to minimum legal requirements; (2) identify any further measures, if necessary, to avoid non-compliance; and, (3) determine optimum solutions which go beyond the legal minima. This legal impact assessment needs to consider the possible compliancy issues raised from a number of relevant legal areas e.g. data protection law and intellectual property law. Legal risk management (i.e. the critical evaluation of possible legally protected interests) is an essential part of a practising lawyer's role [104].[60] However, legal risk management should not be conducted in isolation, but in consultation with other key technical stakeholders (e.g. designers, architects, developers). Individuals and organisations should be actively considering legally protected interests and how to manage them throughout the lifecycle of an ICT platform (e.g. through OPTET's threat and control model). Individuals and organisations should consider what legal assessment model best suits its organisation (taking into account any mandatory obligations e.g. DPIAs) to ensure that the model is transparent and accountable. Independent review is crucial for ensuring the integrity of any legal impact assessment.

(4) Disclosing and signposting legal compliancy and premium trustworthiness features

A key part of an evidence-based approach is signposting to those directly involved with ICT platform design, development, and deployment, end-users and regulatory authorities that an ICT system has reached a level of trustworthiness. This may be communicated to key stakeholders through certification seals (e.g. DTwC), published legal assessment reports, transparent policies and business credentials. Highlighting an authoritative point of contact is important for this on-going dialogue, as an opportunity for feedback.

4.6.2. The model: OPTET-LIM


OPTET Legal Integration Model (OPTET-LIM)
Improved legal integration as an organisational practice
i. Design
ii. Development
iii. Certification
iv. Distribution + Deployment
v. Maintenance
① ② ③
① ② ③
① ② ③ ④
① ② ③ ④
① ② ③ ④
OPTET Lifecycle
A. Interdisciplinary dialogue
+
B. Audit trail
Legal Integration Requirements

[60] For further background information and definitions pertaining to legal risk management see [214]. There are also a number of automated legal risk management systems focused on legal threat modelling (e.g. Legal CORAS – a legal extension to a security and threat modelling language [216]). However, in contrast with technical risk management, there appears to be no agreed standard methodology for legal risk management [215, p. 52].

Category A: On-going interdisciplinary dialogue

① **Raise legal literacy:** There is a need to increase legal knowledge amongst non-legal stakeholders from the preliminary stages of trustworthiness application design and development through greater access to legal expertise and high quality legal information (e.g. more opportunities for engagement and collaboration, training activities, and authoritative soft law instruments).

② **Access to accurate, timely and reliable legal information:** There is a need to identify pertinent hard and soft legal measures from the preliminary stages of trustworthiness application design and development through timely and reliable legal information.

Category B: A robust audit trail

③ **Legal impact assessment:** There is a need to: (1) verify that the specific application conforms to minimum legal requirements; (2) identify any further measures, if necessary, to avoid non-compliance; and, (3) determine optimum solutions which go beyond the legal minima. This should take place from the preliminary stages of trustworthiness application design and development.

④ **Disclosing and signposting legal compliancy and premium trustworthiness features:** In order for end users to make an informed decision about whether to use a specific application, there is a need to indicate that the application released in the trustworthiness marketplace is legally-compliant and, potentially, offers premium trustworthiness features.

4.6.3. Improved legal integration across the OPTET Lifecycle

i. Legal integration within the design phase

During the first phase of the OPTET lifecycle, designers design their trustworthy application and build a Design Time Trustworthiness Model (DTTM) by following the principles of TWbyD. In order to create a robust DTTM, at a basic level, key stakeholders need to: (1) derive system requirements and subsequent trustworthiness attributes; and, (2) examine relevant threats and where necessary highlight the relevant controls that are able to mitigate those threats. First, it is important that the system requirements and trustworthiness attributes take into account any related legal requirements (e.g. a mechanism for explicit consent where handling extremely sensitive personal data). Second, it is crucial that the relevant threats and controls under examination allow for some form of legal risk management i.e. examination of (potential) legally protected interests, the potential consequences of non-compliance, and how such legal risks could be mitigated. Third, key stakeholders need to begin a legal impact assessment which records the decision-making process. For instance, due to limited funding, time and/or resources, it might not be possible to apply the most robust control to mitigate a legal risk. To ensure legal compliance, another moderately robust legal control might be selected instead. In consequence, there is a need to ensure a proficient level of legal literacy amongst all key stakeholders involved with this earliest phase of the OPTET lifecycle. This is further achieved through access to accurate, timely and reliable legal information in order to ensure that key stakeholders are up-to-date with the latest legal developments.

ii. Legal integration within the development phase

At the development stage metrics will be derived to test the trustworthiness attributes and system requirements in order to develop trustworthy software for the trustworthy ICT platform in question. Again, a proficient level of legal literacy and access to accurate, timely and reliable legal information are required in order to ensure that the developed software is legally compliant and mitigates legal risk. This information needs to feed into the on-going legal impact assessment.

iii. Legal integration within the certification phase

The certification phase results in the creation of the Digital Trustworthiness Certification (DTwC) which verifies the development of the system. It is also useful here to scrutinise and signpost legal compliancy, controls, risks and premium options via some form of legal compliancy certification. For this review to be effective, stakeholders need to have proficient legal understanding, access to accurate, timely and reliable legal information, and legal risk management. Again, the certification results need to be recorded as part of the on-going legal impact assessment.

iv. Legal integration within the distribution and deployment phase

During this stage, the particular ICT platform is announced to the TW Market Place. This is a crucial point for legal impact assessment: to ensure that there are no outstanding legal issues before distribution and deployment.

v. Legal integration within the maintenance phase

During this phase, the normal operation of the running trustworthy application is monitored pursuant to the DTWC. It is important that the interdisciplinary dialogue and robust audit trial are sustained to make sure if any (legal) complications arise they are dealt with effectively, and the ICT platform keeps up-to-date with any pertinent legal developments.

4.7. Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) Regulation

4.7.1. Electronic related trust services: eSignatures Directive to eIDAS

In theory, electronic related trust services that facilitate e-authentication and e-identification – such as electronic seals and electronic time stamps – are mechanisms by which end users can authenticate ICT platform providers and their assets (e.g. a trustworthiness application) as genuine. As a result, end users can avoid untrustworthy transactions e.g. using plagiarised and/or fraudulent assets from untrustworthy sources. Jos Dumortier and Niels Vandezande [105, p. 568] identify this "legal certainty" as crucial to enhancing trust in both commercial and non-commercial transactions online. However, in practice, many online transactions are currently completed by clicking an on-screen button (e.g. "I agree") rather than through the use of more robust electronic trust related services (e.g. electronic signatures) [105, p. 568].[61] In consequence, many online interactions between end users and ICT platform providers are without robust e-authentication and e-identification, and therefore lack legal certainty. As the number of online transactions increase – many of which will be of a sensitive nature – greater use needs to be made of these more robust electronic trust related services [106, p. 110].

Regrettably, the long-standing eSignatures Directive 1999/93/EC – the former key legal framework for electronic related trust services – provides for "imperfect and incomplete" [107, p. 9] harmonisation across EU member states; which has resulted in a fragmented market. For instance, electronic signatures are "virtually unused" [106, p. 110] outside of closed public key frameworks such as e-banking.[62] Furthermore, given this Directive's core focus on electronic signatures, it overlooks other crucial electronic related trust services e.g. time stamps and electronic seals [106, p. 111]. In consequence, on 23 July 2014, the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) Regulation (EU) No 910/2014 [9] was adopted

[61] These electronic trust services re-version traditional and familiar pre-digital evidential methods for the digital age, e.g. hand written to electronic signatures and wax to electronic seals [105, p. 568].

[62] As Aaron K. Martin and Norberto Nuno Gomes de Andrade [224, p. 721] state: *"[t]he idea was fairly straightforward: establish a framework for electronic signatures (eSignatures) that would facilitate their use within the European internal market. Nevertheless, more than a decade later it is notorious that this Directive has largely failed to accomplish this objective, generating little interest and traction."*

by the European Parliament and the European Council [108]. The eIDAS Regulation supersedes the eSignatures Directive 1999/93/EC – which will be repealed on 1 July 2016 (pursuant to Article 50 of the eIDAS Regulation).

The European Commission outlines the main purpose of the eIDAS Regulation in its impact assessment report [107]: "[t]he objective is to enable secure and seamless electronic interactions between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services and electronic commerce in the EU, thus creating trust in electronic transactions in the internal market."[63] For instance, where possible, EU citizens will be able to utilise their electronic identities (eIDs)[64] for cross-border e-authentication and e-identification in other member states through the principle of "mutual recognition" (under Article 6 of the eIDAS Regulation). In addition, the eIDAS Regulation introduces the legal concept of trust services [109] and promotes the use of qualified trust service providers[65] (under Chapter III).[66] Audit – an important aspect of legal integration – is also an important feature of the eIDAS Regulation (see paragraph (15) and Chapter III).

P.P. Polanski [110, pp. 2-3] identifies five key factors which separate eIDAS from the eSignatures Directive (refer to article for full information): (1) as a regulation it provides "unified rules" rather than minimum harmonisation across member states; (2) it has a "much broader scope" not only focusing on electronic signatures but other trust services (i.e. electronic seals, electronic time stamps, electronic registered delivery services, website authentication, and electronic documents[67]); (3) it introduces a new limitation[68] where, e.g., it does not apply to exclusive e-banking or e-

[63] For instance, the eIDAS Regulation should enable: *"students to enrol at university online [in another member state]; citizens to fill on-line tax returns in another EU country; and businesses to participate electronically in public calls for tenders across the EU.* [221, p. 284]" – see [107, pp. 8-9] for full scenarios; for more information concerning the potential impact of eIDAS on university enrolment see [222] and [223].

[64] Where eIDs are available e.g. the UK does not have a national identity card scheme, but the UK government have established Gov.UK Verify [225] an eID for online UK government services. Furthermore, the STORK project (Security Identity across Borders Linked) [227] set to establish: *"a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID."* In addition, the STORK 2.0 project [226]: *"builds on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities."*

[65] A 'trust service provider' is defined by Article 3(19) of eIDAS as: "*a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider".* A 'qualified trust service provider' is defined by Article 3(20) of eIDAS as: "*a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body".*

[66] In order to confirm their compliance with the eIDAS Regulation, qualified trust service providers must be audited at least every two years by a conformity assessment body* (pursuant to Article 20(1)). Furthermore, the supervisory body is able to request a conformity assessment at any time (pursuant to Article 20(2)) and member states have to: *"establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them"* (pursuant to Article 22(1)). *A 'conformity assessment body' is defined by Article 3(18) of eIDAS as: "*a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides".*

[67] Electronic signatures – under Articles 25-34; electronic seals – under Articles 35-40; electronic time stamps – under Articles 41-42, electronic registered delivery services – under Articles 43-44; website authentication – under Article 45; and electronic documents – under Article 46.

[68] Article 2(2) of the eIDAS Regulation states: *"[t]he Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants".*

commerce payment systems; (4) its implementation will depend on secondary legislation outlining technical and organisational measures; and, (5) it provides a more detailed legislative framework than its current international counterparts.

4.7.2. eIDAS: some grey areas

The eIDAS regulation is advocated as the newest and leading legislative instrument to promote trust in the online environment. Its successful implementation is set to largely depend on its implementing acts, other soft law measures such as policy, standards, and effective communication; which are being developed by the eIDAS Task Force (eIDAS Legislative Team) [111]. Despite appearing to be "largely unnoticed" [110, p. 2] thus far, it seems likely that this could change through the aforementioned strategy providing for further support and communication. Furthermore, member states will be encouraged to produce useful eIDAS schemes for the digital single market.

However, a number of key grey areas are already starting to emerge, and mirror some of the key grey areas already raised in respect of the GDPR. First, the eIDAS Regulation incorporates the principle of PbyD under Article 12(3)(c): "[t]he interoperability framework shall meet the following criteria […] (c) it facilitates the implementation of the principle of privacy by design […]." This inclusion of PbyD may help to draw further attention to the value-by-design approach. It also illustrates how value-by-design is beginning to feature across a number of legislative instruments e.g. the eIDAS Regulation and the proposed GDPR. However, a point that is interesting to note, is that Article 12(3)(c) of the eIDAS Regulation uses the expression 'PbyD' in contrast to Article 23 of the proposed GDPR which utilises 'DPbyD'. Is PbyD used as a synonym for DPbyD, or does it allude to a separate value-by-design approach? Furthermore, as PbyD has also been understood in many different ways, it is unclear what approach the eIDAS regulation supports. It will be of interest to observe whether any of the secondary acts and other materials clarify this position.

Second, under paragraph (27) of the pre-amble to the eIDAS Regulation it states 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."

Once more, it will be of interest to pay attention to the secondary legislation and other soft law guidance to see if this techno-neutrality is upheld in practice or whether *de facto* standards emerge that (unintentionally) infringe on this neutral position. Importantly, as a result of this statement it is not entirely clear whether techno-regulation has really a place within the Future Internet environment.

Third, while arguably the eIDAS regulation provides a useful mechanism to boost e-identification and e-authentication services and therefore trustworthiness attributes, these are only two aspects amongst many for optimising trust and trustworthiness. In this sense, OPTET provides a more comprehensive approach to trust and trustworthiness that extends beyond e-identification and e-authentication.

4.7.3. TWbyD: providing 'trustworthy' electronic related trust services

Electronic trust services are not one-hundred percent infallible, as the case of DigiNotar[69] proves [105, p. 572]. To minimise the risk of their misuse and abuse (e.g. through cyber-attack), it is of

[69] DigiNotar was a web security firm appointed by the Dutch government to issue Secure Sockets Layer (SSL) certificates for its electronic services (e.g. tax returns). In July 2011, a cyber-attack took place which resulted in over 500 fake

critical importance that ICT platforms executing electronic identification and trust services should be trustworthy by their very design. Assuming the eIDAS Regulation is already acquainted with value-by-design (i.e. Article 12(3)(c) refers to PbyD), the overall OPTET approach is particularly well-positioned to assist with the future development of electronic identification and trust service policy and architecture. In consequence, the future development of electronic identification and trust service policy and architecture is one significant way in which the project (i.e. future work) may be taken forward to potentially: (1) ensure the trustworthiness of eIDAS through TWbyD; and, (2) broaden the scope of eIDAS beyond e-authentication and e-identification to other trustworthiness attributes.

certificates being issued, and subsequent revocation of all DigiNotar certificates by the Dutch government. For more information see [105, p. 572] and [220].

5. Conclusion and future work

5.1.1. *The Future Internet and the law*

The concept of the Future Internet offers a compelling, yet open-ended, representation of a matured digital age. While the necessary infrastructure, level of standardisation and other requirements are yet to be realised, the early stages of a possible Future Internet environment already appear to be surfacing e.g. through Internet of Things technologies and cloud services.[70] Given the wide-range of hard law and soft law instruments at a law maker's disposal and the global, cross-jurisdictional nature of the digital age, any possible legal approach is likely to be multi-faceted, complex and comprised of an array of hard and soft legal measures produced via regulatory, co-regulatory and self-regulatory fora. As well as acquiring new legal measures, a Future Internet governance framework will inherit those measures and principles which are longstanding. The success of a set of legal measures will rely as much on their scope and level of power as the extent in which they are effectively implemented and interpreted (by the courts and all other key stakeholders) within a Future Internet environment.

A key grey area raised in section 4.4 is the potential role of techno-legal measures within a governance framework for the Future Internet environment. Therefore a significant philosophical question for computer scientists, social scientists, economists, legal experts and other key stakeholders to contemplate is: **to what extent techno-legal measures will have a role in the overall approach to a trusted Future Internet, and whether this type of approach is justified?** It will be of further interest to observe whether European ICT law continues to develop as a set of unifying rules (e.g. the eIDAS Regulation [110, p. 2]) rather than as a means for minimal harmonisation.

5.1.2. *Value-by-design and the role of the law*

'What is the role of the law in a value-by-design approach to a trusted Future Internet environment?'

Section 4 has further shown that the GDPR is likely to have the foremost role in the data protection approach to a trusted Future Internet (principally within Europe). It will necessitate stronger internal procedures (where necessary) for handling and processing personal data [38, p. 175]. The GDPR clearly supports a value-by-design approach (i.e. DPbyD) to ICT platform design and development. Furthermore, the eIDAS Regulation also places a value-by-design approach (i.e. PbyD) within a legal framework that explicitly aims to promote online trust. This expanding legal portfolio appears to illustrate that, in the areas of data protection and online trust at least, EU law is pursuing certain value-by-design approaches through hard law instruments.

While this legislative incentive for value-by-design is welcomed, sections 4.4-4.5 revealed a variety of weaknesses of the DPbyD approach, the most significant of these issues being a lack of

[70] For instance, Internet of Things devices and cloud computing services are available for deployment; and, in some instances, have already triggered privacy concerns [158]. One such example is the voice recognition software employed with the Samsung Smart TV that is able to record and transmit personal conversations; this personal data has the potential to be used by unauthorised third parties [184]. In some cases, there is growing trepidation that greater deployment of such technologies could further facilitate active monitoring, surveillance, profiling, increased opportunities for data leakage and re-usage of personal data for unknown and unforeseen purposes by unauthorised entities [159, p. 68]. Also refer to [187] for further information about a potential 'looming IoT backlash'.

guaranteed interdisciplinary dialogue and accountability. In comparison, TWbyD is shown to be a more robust value-by-design approach. It largely addresses the weaknesses that arise from the proposed legal framework by offering a broader, interdisciplinary and more systematic approach.

EU ICT law will have a role in facilitating a value-by-design approach – namely DPbyD (Article 23 of the GDPR) and PbyD (Article 12(3)(c) of the eIDAS Regulation.) Despite this, it is too early to comment on how this role will unfold in practice. For instance, it is not yet known in which ways the law will be interpreted and implemented (e.g. the GDPR has not yet entered force), how a Future Internet environment will develop and mature, or to what extent other non-legally binding value-by-design approaches (e.g. TWbyD) will prove popular. It will be of interest to observe how this legal situation develops over the coming years, and whether legal support for the value-by-design approach will continue to increase through further hard and soft legal instruments and from other legal areas and jurisdictions.

5.1.3. The need for improved legal integration: OPTET-LIM

Although self-evident, the implementation of a value-by-design approach is ineffective without the necessary interdisciplinary knowledge bases, good communication and skilled experts to implement it. Section 4.6 therefore raised the need for improved legal integration through the OPTET-LIM. While improved legal integration is no panacea, it should be viewed nonetheless as a crucial component of both TWbyD and the overall, combined technological, socio-cultural, economic, political, ethical and legal approach to a trusted Future Internet. The OPTET-LIM therefore provides a holistic and re-usable framework for implementing value-by-design to build on. Furthermore, TWbyD has been shown to be a useful reference point for future acts and guidance on the GDPR DPbyD approach.

5.1.4. Electronic identification and trust service policy and architecture

The future development of electronic identification and trust service policy and architecture was identified as a potential area of future significance for OPTET in section 4.7. The successful implementation of the eIDAS Regulation is set to largely depend on its implementing acts, other soft law measures such as policy, standards, and effective communication [111]. Other trust related projects are already being used to formulate these supporting frameworks [111]. Hence there is also an opportunity for the OPTET knowledge base to be taken forward in order to further enrich the "positive environment for the acceptance and wide uptake of the new legislative framework" [111] which the eIDAS Task Force (eIDAS Legislative Team) are seeking to create. OPTET could potentially enhance the future development of electronic identification and trust service policy and architecture through: (1) the provision of robust interdisciplinary understanding of the significant socio-economic, legal and technological aspects of trust and trustworthiness – and hence the promotion of valuable interdisciplinary dialogue; (2) the application of OPTET methodologies and technologies that enable evidence-based trustworthiness management – to therefore ensure the trustworthiness of eIDAS through TWbyD; and, (3) broadening the scope of eIDAS beyond e-authentication and e-identification to other trustworthiness attributes that are likely to further optimise trust both now and as the digital age matures.

6. References

[1] O. C. «D2.3 – Socio-economic evaluation of trust and trustworthiness,» 2014.

[2] OPTET Consortium, «D2.1: Socio-economic requirements for trust and trustworthiness,» OPTET – 317631, FP7-ICT-2011-8, 2014.

[3] O. C. «D2.2: Socio-economic models for trust and trustworthiness evaluation,» 2014.

[4] O. C. «D2.4: Socio-economic evaluation of trust and trustworthiness,» 2015.

[5] C. e. a. Derman, «Optimal system allocations with penalty costs.,» *Management Science,* n. 23.4, pp. 399-403, 1976.

[6] OPTET Consortium , «D3.1: Initial concepts and abstractions to model trustworthiness,» OPTET – 317631, FP7-ICT-2011-8, 14 June 2013.

[7] F. Di Cerbo, P. Bisson, A. Hartman, S. Keller, P. H. Meland, M. Moffie, N. G. Mohammadi, S. Paulus e S. Short, «Towards Trustworthiness Assurance in the Cloud,» in *Cyber security and privacy: trust in the digital world and cyber security and privacy EU forum 2013, Brussels, Belgium, April 2013, revised selected papers*, Springer Berlin Heidelberg, 2013, pp. 3-15.

[8] «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) /* COM/2012/011 final - 2012,» 25 January 2015. [Online]. Available: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011. [Consultato il giorno 17 August 2015].

[9] European Parliament and European Council, «Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) Regulation (EU) No 910/2014,» 23 July 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. [Consultato il giorno 1 October 2015].

[10] P. Jäppinen, R. Guarneri e L. M. Correia, «An applications perspective into the Future Internet,» *Journal of Network and Computer Applications,* vol. 36, n. 1 , p. 249–254, 2013.

[11] Digital agenda for Europe: a Europe 2020 initiative, «Future Internet,» European Commission (EC) , [Online]. Available: http://ec.europa.eu/digital-agenda/en/future-internet. [Consultato il giorno 4 August 2015].

[12] E. Townsend, «UK Future Internet Strategy Group: Future Internet Report,» Researched and authored by Eddie Townsend on behalf of the ICT KTN, Innovate UK (formerly the Technology Strategy Board (TSB)) , 2011.

[13] M. Caporuscio e C. Ghezzi, «Engineering Future Internet applications: The Prime approach,» *Journal of Systems and Software,* vol. 106, pp. 9-27, 2015.

[14] Y. Lu, M. Motani e W.-C. Wong, «The User-Context Module: A New Perspective on Future Internet Design,» *Procedia Computer Science,* vol. 5, p. 280–287, 2011.

[15] European Commission (EC), «Monitoring the application of Union law,» 8 June 2015. [Online]. Available: http://ec.europa.eu/atwork/applying-eu-law/index_en.htm. [Consultato il giorno 4 August 2015].

[16] European Commission (EC) , «Legislation,» 21 January 2015. [Online]. Available: http://ec.europa.eu/legislation/index_en.htm. [Consultato il giorno 5 August 2015].

[17] European Commission (EC), «Regulations, directives and other acts,» 17 July 2015. [Online]. Available: http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm. [Consultato il giorno 4 August 2015].

[18] K. C. Wellens e G. M. Borchardt, «Soft law in European Community law,» *European Law Review,* vol. 14, n. 5, pp. 267-321, 1989.

[19] E. Ferran e K. Alexander, «Can soft law bodies be effective? The special case of the European Systemic Risk Board,» *European Law Review,,* vol. 35, n. 6, pp. 751-776, 2010.

[20] O. Stefan, «Hybridity before the court: a hard look at soft law in the EU competition and state aid case law,» *European Law Review,* vol. 37, n. 1, pp. 49-69, 2012.

[21] A. T. Guzman, «The design of international agreements,» *European Journal of International Law,* vol. 16, n. 4, pp. 579-612, 2005.

[22] H. Marjosola, «Regulating financial markets under uncertainty: the EU approach,» *European Law Review,* vol. 39, n. 3, pp. 338-361, 2014.

[23] H.-W. Liu, «International Standards in Flux: A Balkanized ICT Standard-Setting Paradigm and Its Implications for the WTO,» *Journal of International Economic Law,* vol. 17, n. 3, pp. 551-600, 2014 (Available via SSRN).

[24] International Organization for Standardization (ISO), «ISO/IEC 27018:2014 – Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,» 1 August 2014. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498. [Consultato il giorno 5 August 2015].

[25] S. Curtis, «Should you be worried about the cloud?,» *The Telegraph (Online),* 18 February 2015.

[26] Osbourne Clarke Publications, «New ISO standard for cloud providers,» 28 October 2014. [Online]. Available: http://www.osborneclarke.com/connected-insights/publications/new-iso-standard-cloud-providers/#sthash.KIG4CeaC.dpuf. [Consultato il giorno 5 August 2015].

[27] European Commission (EC), «Digital Agenda for Europe: A Europe 2020 Initiative: European Cloud Strategy,» 27 February 2015. [Online]. Available: http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy. [Consultato il giorno 5 August 2015].

[28] B. Smith, «Microsoft adopts first international cloud privacy standard,» Microsoft on the Issues Blog, 16 February 2015. [Online]. Available: http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/. [Consultato il giorno 5 August 2015].

[29] T. Erbay, «Dropbox for Business achieves ISO 27018 certification, an emerging international cloud standard for privacy and data protection,» Dropbox for Business Blog, 18 May 2015. [Online]. Available: https://blogs.dropbox.com/business/2015/05/dropbox-for-business-iso-27018/. [Consultato il giorno 5 August 2015].

[30] EY CertifyPoint , «About EY CertifyPoint,» [Online]. Available: http://www.ey.com/GL/en/Services/Specialty-Services/CertifyPoint. [Consultato il giorno 5 August 2015].

[31] L. Tonsager, «International Standard Could Reshape Cloud Privacy,» *Law360: New York,* pp. 1-3, 21 October 2014 (Available via SSRN).

[32] Kemp IT Law: IT+ Blog, «The Growing Role of Standards in Cloud Contracts – Some Perspectives on ISO 27018,» 26 October 2014. [Online]. Available: http://www.kempitlaw.com/the-growing-role-of-standards-in-cloud-contracts-some-perspectives-on-iso-27018/. [Consultato il giorno 5 August 2015].

[33] M. Webber, «A new ISO standard for cloud computing,» fieldfisher: Privacy and Information Law Blog, 5 November 2014. [Online]. Available: http://privacylawblog.fieldfisher.com/2014/a-new-iso-standard-for-cloud-computing. [Consultato il giorno 5 August 2015].

[34] I. Kroener e D. Wright, «A Strategy for Operationalizing Privacy by Design,» *The Information Society,* vol. 30, n. 5, pp. 355-365, 2014.

[35] Official Journal of the European Union, L 281, 23/11/1995 P. 0031 – 0050, «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,» 24 October 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. [Consultato il giorno 11 August 2015].

[36] Information Commissioner's Office (ICO), «Big data and data protection,» 20140728, Version: 1.0, 2014.

[37] C. Rooney, «Legislative Comment – Things to do to prepare for the new Regulation,» *Privacy & Data Protection,* vol. 13, n. 3, pp. 5-7, 2013.

[38] W. J. Maxwell, «Legislative Comment – Data privacy: the European Commission pushes for total harmonisation,» *Computer and Telecommunications Law Review,* vol. 18, n. 6, pp. 175-176, 2012.

[39] European Parliament , «European Parliament legislative resolution the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)),» 12 March 2014. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN. [Consultato il giorno 24 August 2015].

[40] Presidency, Council of the European Union, «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) ST 15395 2014 INIT,» 19 December 2014. [Online]. Available: http://www.consilium.europa.eu/register/en/content/out/?&typ=ENTRY&i=SMPL&DOC_ID=ST-15395-2014-INIT. [Consultato il giorno 24 August 2015].

[41] European Commission (EC), «Memo: Progress on EU data protection reform now irreversible following European Parliament vote,» 12 March 2014. [Online]. Available: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm. [Consultato il giorno 17 August 2015].

[42] B. Treacy, «Formalising the role of the DPO - the practical consequences,» *Privacy & Data Protection,* vol. 12, n. 3, pp. 3-5, 2012.

[43] R. Imperiali , «The Data Protection Compliance Program,» *Journal of International Commercial Law and Technology,* vol. 7, n. 3, p. 285–288, 2012.

[44] M. Warman, «EU Privacy regulations subject to 'unprecedented lobbying',» *The Telegraph (Online),* 8 February 2012.

[45] S. Islam, H. Mouratidis e J. Jürjens, «A framework to support alignment of secure software engineering with legal regulation,» *Software & Systems Modeling,* vol. 10, n. 3, pp. 369-394, 2011.

[46] K. Wuyts, R. Scandariato e W. Joosen, «Empirical evaluation of a privacy-focused threat modeling methodology,» *Journal of Systems and Software,* vol. 96, pp. 122-138, 2014.

[47] AEGIS Report by AEGIS Systems Ltd and Machina Research, 2606/OM2M/FR/V2 , «M2M Application Characteristics and Their Implications for Spectrum,» Final Report for Ofcom, 2014.

[48] M. Hildebrandt e L. Tielemans , «Data protection by design and technology neutral law,» *Computer Law & Security Review,* vol. 29, n. 5, p. 509–521, 2013.

[49] B.-J. Koops e R. Leenes, «Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law,» *International Review of Law, Computers & Technology,* vol. 28, n. 2, pp. 159-171, 2014.

[50] A. Cavoukian, «Privacy by Design,» 27 January 2009. [Online]. Available: https://www.privacybydesign.ca/index.php/paper/privacy-by-design/. [Consultato il giorno 4 August 2015].

[51] D. Le Métayer, «Privacy by Design: Formal Framework for the Analysis of Architectural Choices,» in *Proceedings of the third ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, 2013.

[52] J. van Rest, D. Boonstra, M. Everts, M. van Rijn e R. van Paassen , «Designing Privacy-by-Design,» in *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*, Springer Berlin Heidelberg, 2014, pp. 55-72.

[53] M. Halper, «Isabelle Falque-Pierrotin: Privacy Needs to Be the Default, Not an Option,» *Wired,* 25 June 2015.

[54] R. Gellert e S. Gutwirth, «The legal construction of privacy and data protection,» *Computer Law & Security Review,* vol. 29, n. 5, p. 522–530, 2013.

[55] M. van Lieshout, L. Kool, B. van Schoonhoven e M. de Jonge, «Privacy by Design: an alternative to existing practice in safeguarding privacy,» *info,* vol. 13, n. 6, pp. 55-68, 2011.

[56] I. Rubinstein, «Regulating Privacy by Design,» *Berkeley Technology Law Journal,* vol. 26, pp. 1409-1456, 2012 (Available via SSRN).

[57] J. I. Hong, J. D. Ng, S. Lederer e J. A. Landay , «Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems,» in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS)*, Cambridge MA, 2004.

[58] M. Hildebrandt e L. Tielemans, «Data protection by design and technology neutral law,» *Computer Law & Security Review,* vol. 29, n. 5, p. 509–521, 2013 .

[59] M. C. Oetzel e S. Spiekermann, «A systematic methodology for privacy impact assessments: a design science approach,» *European Journal of Information Systems,* vol. 23, p. 126–150, 2014.

[60] L. Costa e Y. Poullet, «Privacy and the regulation of 2012,» *Computer Law & Security Review,* vol. 28, n. 3, p. 254–262, 2012.

[61] C. Knobel e G. C. Bowker, «Viewpoints: Computing Ethics – Values in Design,» *Communications of the ACM,* vol. 54, n. 7, pp. 26-28, 2011.

[62] A. Maughan, «The Internet of Things: a lawyer's guide,» *Computers and Law,* vol. 25, n. 3, pp. 17-18, 2014.

[63] N. Manders-Huits, «What Values in Design? The Challenge of Incorporating Moral Values into Design,» *Science and Engineering Ethics,* vol. 17, n. 2, pp. 271-287, 2011.

[64] P. Sengers, K. Boehner , S. David e J. . Kaye , «Reflective design,» in *Proceedings of the 4th decennial conference on critical computing: between sense and sensibility (CC)*, Aarhus, 2005.

[65] M. Pocs, «Will the European Commission be able to standardise legal technology design without a legal method?,» *Computer Law & Security Review,* vol. 28, pp. 641- 650, 2012.

[66] X. Konarski, D. Karwala, H. Schulte-Nölke e S. Charlton, «Reforming the Data Protection Packge Study,» Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy, European Parliament, IP/A/IMCO/ST/2012-02, PE 492.431, Publications Office, 2012.

[67] E. Goodman, «Design and Ethics in the Era of Big Data,» *Interactions,* vol. 21, n. 3, pp. 22-24, 2014.

[68] O. Whitcroft, «Apps and privacy: Part 2: playing a part,» *Privacy & Data Protection,* vol. 14, n. 4, pp. 3-6, 2014.

[69] S. S. Shapiro, «Privacy By Design: Moving From Art to Practice,» *Communications of the ACM,* vol. 53, n. 6, pp. 27-29, 2010.

[70] L. Danagher, «An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?,» *European Journal of Law and Technology,,* vol. 3, n. 3, 2012.

[71] C. Cuijpers, N. Purtova e E. Kosta, «Data Protection Reform and the Internet: The Draft Data Protection Regulation,» in *Research Handbook on EU Internet Law* , Edward Elgar, 2014, pp. 1-20 (SSRN Version).

[72] I. S. Rubinstein, «Big Data: The End of Privacy or a New Beginning?,» *International Data Privacy Law ,* pp. 1-14 (SSRN Version), 2013.

[73] S. Spiekermann, «Viewpoint: The Challenges of Privacy by Design,» *Communications of the ACM,* vol. 55, n. 7, pp. 38-40, 2012.

[74] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirte e S. Schiffner, «Privacy and Data Protection by Design – from policy to engineering,» European Union Agency for Network and Information Security (ENISA), Heraklion, 2014.

[75] S. Spiekermann e L. F. Cranor, «Engineering Privacy,» *IEEE Transactions on Software Engineering,* vol. 35, n. 1, pp. 67-82, 2009.

[76] J.-H. Hoepman, «Privacy Design Strategies,» in *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, Springer Berlin Heidelberg, 2014, pp. 446-459.

[77] S. Gürses, C. Troncoso e C. Diaz, «Engineering Privacy by Design,» *Computers, Privacy & Design,* 2011.

[78] S. Lahlou e F. Jegou, «European disappearing computer privacy design guidelines, Version 1.1,» 2004 (Discussion Paper, Version 1.1. Ambient Agora-s IST 2000-25134, version 1.1. Ambient Agoras. Unpublished. Available in LSE Research Online: June 2011.). [Online]. Available: http://eprints.lse.ac.uk/33125/. [Consultato il giorno 27 August 2015].

[79] «7 Foundational Principles,» [Online]. Available: https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/. [Consultato il giorno 4 August 2015].

[80] J. Luna, N. Suri e I. Krontiris, «Privacy-by-design based on quantitative threat modeling,» in *Proceedings of the 7th International Conference on Risk and Security of Internet and Systems (CRiSIS)*, Cork, Republic of Ireland, 2012.

[81] K. Kaye, «'Privacy-by-Design' Is Crucial, but Not Easy or Cheap,» *Advertising Age,* 6 October 2014.

[82] D. K. Mulligan e K. A. Bamberger, «Viewpoints: privacy and security – what regulators can do to advance privacy through design,» *Communications of the ACM,* vol. 56, n. 1), pp. 20-22, 2013.

[83] B. Stewart, «Privacy impact assessment towards a better informed process for evaluating privacy issues arising from new technologies,» *Privacy Law and Policy Reporter,* vol. 5, n. 8, p. 147, 1999.

[84] D. Tancock, S. Pearson e A. Charlesworth, «A Privacy Impact Assessment Tool for Cloud Computing,» in *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)* , Indianapolis, IN, USA, 2010 .

[85] S. Pritchett, «Using privacy impact assessments,» *Privacy and Data Protection,* vol. 10, n. 6, pp. 7-9, 2010.

[86] Information Commissioner's Office (ICO), «Conducting Privacy Impact Assessments: Code of Practice,» 20140225, Version: 1.0, 2014.

[87] D. Wright, «The state of the art in privacy impact assessment,» *Computer Law & Security Review,* vol. 28, n. 1, p. 54–61, 2012.

[88] B. Treacy, «Expert Comment,» *Privacy & Data Protection,* vol. 14, n. 4, p. 2, 2014.

[89] M. Salgado, «PIAs and privacy by design - using them to your advantage,» *Privacy & Data Protection,* vol. 13, n. 8, pp. 3-5, 2013.

[90] L. Costa, «Privacy and the precautionary principle,» *Computer Law & Security Review,* vol. 28, n. 1, p. 14–24, 2012.

[91] S. Pritchett, «Legislative Comment - Data protection impact assessments: look before you leap,» *Privacy & Data Protection,* vol. 12, n. 6, pp. 11-14, 2012.

[92] F. Harrison, «Data protection and surveillance technologies: Part 1 - ANPR,» *Privacy & Data Protection,* vol. 15, n. 3, pp. 7-9, 2015.

[93] D. Wright, R. Finn e R. Rodrigues, «A Comparative Analysis of Privacy Impact Assessment in Six Countries,» *Journal of Contemporary European Research,* vol. 9, n. 1, p. 160-180, 2013.

[94] D. Wright e C. Raab, «Privacy principles, risks and harms,» *International Review of Law,Computers & Technology,* vol. 28, n. 3, pp. 277-298, 2014.

[95] D. Wright, «Making Privacy Impact Assessment More Effective,» *The Information Society,* vol. 29, n. 5, pp. 307-315, 2013.

[96] European Commission, «Commission Staff Working Paper: Impact Assessment,» 25 January 2012. [Online]. Available: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm. [Consultato il giorno 4 September 2015].

[97] P. De Hert e V. Papakonstantinou , «The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals,» *Computer law & Security Review ,* vol. 28, n. 2, p. 130–142, 2012.

[98] J. Cline, «Will the EU Privacy Reform Boost Privacy Seal Adoption?,» *International Association of Privacy Professionals (IAPP),* 13 April 2012.

[99] European Privacy Seal: EuroPriSe, «Welcome!,» [Online]. Available: https://www.european-privacy-seal.eu/EPS-en/Home. [Consultato il giorno 19 August 2015].

[100] European eCommerce Association (EMOTA), «Press release: European Trust Mark for online shopping launched today Commissioner Jourova welcomes initiative to provide confidence to European consumer,» 1 July 2015. [Online]. Available: http://www.emota.eu/#!publications/c1351. [Consultato il giorno 19 August 2015].

[101] OPTET Consortium , «D3.2 – Initial trustworthiness-by-design process and tool support,» OPTET – 317631, FP7-ICT-2011-8, 11 November 2013.

[102] G. Coraggio, «Internet of Things needs privacy by design,» Lexology, 11 June 2015. [Online]. Available: http://www.lexology.com/library/detail.aspx?g=fcdeb2db-7a5b-4548-8a2c-d07bcbdecb9c. [Consultato il giorno 4 August 2015].

[103] B. Subirana e M. Bain, «Legal Programming,» *Communications of the ACM – Privacy and Security in Highly Dynamic Systems,* vol. 49, n. 9, pp. 57-62, 2006.

[104] T. Mahler, «Tool-supported Legal Risk Management: A Roadmap,» *European Journal of Legal Studies,* vol. 2, n. 3, 2010.

[105] J. Dumortier e N. Vandezande, «Trust in the proposed EU regulation on trust services?,» *Computer Law & Security Review,* vol. 28, n. 5, p. 568–576, 2012.

[106] H. Graux, «Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union,» *Journal of International Commercial Law and Technology,* vol. 8, n. 2, p. 110–117, 2013.

[107] Commission Staff Working Paper, «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,» European Commission , Brussels, 4 June 2012 {SWD(2012) 136 final} {COM(2012) 238 final}.

[108] European Commission (EC), «Digital Agenda fro Europe - A Europe 2020 Initiative: Trust Services and eID,» 30 September 2015. [Online]. Available: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid. [Consultato il giorno 1 October 2015].

[109] Out-law.com, «The EU's proposed new e-identification regime,» August 2012. [Online]. Available: http://www.out-law.com/topics/tmt--sourcing/e-commerce/the-eus-proposed-new-e-identification-regime/. [Consultato il giorno 9 October 2015].

[110] P. P. Polanski , «Towards the single digital market for e-identification and trust services,» *Computer Law & Security Review,* 2015 [In press, corrected proof - last accessed 6 October 2015].

[111] Legislation Team (eIDAS) (Task Force eIDAS), «Electronic identification and trust services (eIDAS): regulatory environment and beyond,» European Commission (EC), [Online]. Available: https://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond. [Consultato il giorno 8 October 2015].

[112] European Commission (EC), «Press Release: Launch of Alliance for Internet of Things Innovation,» 24 March 2015. [Online]. Available: https://ec.europa.eu/digital-agenda/en/news/launch-alliance-internet-things-innovation. [Consultato il giorno 5 August 2015].

[113] European Commission, «The Alliance for Internet of Things Innovation (AIOTI),» 1 July 2015. [Online]. Available: https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti. [Consultato il giorno 13 August 2015].

[114] British Standards Institute (BSI), «Data Protection & Freedom of Information Standards,» 2015. [Online]. Available: http://shop.bsigroup.com/en/Browse-by-Subject/Data-Protection--Freedom-of-Information/?t=r. [Consultato il giorno 12 August 2015].

[115] Body of European Regulators for Electronic Communications (BEREC) , [Online]. Available: http://berec.europa.eu/. [Consultato il giorno 12 August 2015].

[116] EuroCloud (Europe), «'About us',» [Online]. Available: http://www.eurocloud.org/about.html. [Consultato il giorno 13 August 2015].

[117] EuroCloud UK, [Online]. Available: http://www.eurocloud.org.uk/home. [Consultato il giorno 13 August 2015].

[118] European Telecommunications Standards Institute (ETSI), «Connecting Things,» 2015. [Online]. Available: http://www.etsi.org/technologies-clusters/clusters/connecting-things. [Consultato il giorno 12 August 2015].

[119] European Telecommunications Standards Institute (ETSI), «ETSI Cluster Brochures,» 2015. [Online]. Available: http://www.etsi.org/technologies-clusters/white-papers-and-brochures/etsi-cluster-brochures. [Consultato il giorno 12 August 2015].

[120] S. Antipolis, «Cross-sector involvement is key to standards for Internet of Things,» European Telecommunications Standards Institute (ETSI) News, 17 July 2014. [Online]. Available: http://www.etsi.org/news-events/news/808-2014-07-news-release-cross-sector-involvement-is-key-to-standards-for-internet-of-things?highlight=YToxOntpOjA7czoxODoiaW50ZXJuZXQgb2YgdGhpbmdzIjt9. [Consultato il giorno 12 August 2015].

[121] oneM2M, «List of partners in oneM2M,» 2015. [Online]. Available: http://www.onem2m.org/about-onem2m/partners. [Consultato il giorno 12 August 2015].

[122] European Union Agency for Network and Information Security (ENISA) Website , [Online]. Available: https://www.enisa.europa.eu/. [Consultato il giorno 17 September 2015].

[123] International Telecommunication Union (ITU) , «Internet of Things Global Standards Initiative,» [Online]. Available: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Consultato il giorno 13 August 2015].

[124] International Telecommunication Union (ITU), «About ITU,» [Online]. Available: http://www.itu.int/en/about/Pages/default.aspx. [Consultato il giorno 13 August 2015].

[125] oneM2M, [Online]. Available: http://www.onem2m.org/. [Consultato il giorno 12 August 2015].

[126] Online Trust Alliance (OTA), «About us,» [Online]. Available: https://otalliance.org/about-us. [Consultato il giorno 13 August 2015].

[127] Online Trust Alliance (OTA), «Internet of Things: IoT Trust Framework - Security, Privacy & Sustainability,» 11 August 2015. [Online]. Available: https://otalliance.org/initiatives/internet-things. [Consultato il giorno 13 August 2015].

[128] Online Trust Alliance (OTA), «Online Trust Audit and Honor Roll,» 16 June 2015. [Online]. Available: https://otalliance.org/HonorRoll. [Consultato il giorno 13 August 2015].

[129] Organisation for Economic Co-operation and Development (OECD), «About,» [Online]. Available: http://www.oecd.org/about/. [Consultato il giorno 13 August 2015].

[130] Organisation for Economic Co-operation and Development (OECD), «2013 OECD Privacy Guidelines,» [Online]. Available: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. [Consultato il giorno 13 August 2015].

[131] Organization for the Advancement of Structured Information Standards (OASIS), [Online]. Available: https://www.oasis-open.org/. [Consultato il giorno 12 August 2015].

[132] Perinorm, «Welcome to Perinorm,» 3 August 2015. [Online]. Available: https://www.perinorm.com/. [Consultato il giorno 5 August 2015].

[133] British Standards Institute (BSI), «Perinorm,» [Online]. Available: http://shop.bsigroup.com/perinorm. [Consultato il giorno 5 August 2015].

[134] The UK Anonymisation Network (UKAN), «About us,» 2015. [Online]. Available: http://ukanon.net/about-us/. [Consultato il giorno 12 August 2015].

[135] Digital Catapult, «Trust in Personal Data: A UK Review – Following and assessing the UK's journey to becoming a data-driven nation,» 2015.

[136] Personal Data and Trust Network (PDTN), [Online]. Available: http://www.pdtn.org/. [Consultato il giorno 7 August 2015].

[137] Digital Catapult Centre, «Open Call: Trust Framework Initiative,» Innovate UK: Technology Strategy Board, 2015. [Online]. Available: http://www.digitalcatapultcentre.org.uk/open-calls/trust-framework-initiative/. [Consultato il giorno 7 August 2015].

[138] M. Langheinrich, «Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems,» in *Ubicomp 2001: Ubiquitous Computing - International Conference Atlanta Georgia, USA, September 30–October 2, 2001 Proceedings*, Springer Berlin Heidelberg, 2001, pp. 273-291.

[139] E. Yu e L. M. Cysneiros, «Designing for Privacy and Other Competing Requirements,» in *Symposium on Requirements Engineering for Information Security (SREIS)*, Raleigh, North Carolina, USA, 2002.

[140] S. Lahlou, M. Langheinrich e C. Röcker , «Privacy and trust issues with invisible computers,» *Communications of the ACM,* vol. 48, n. 3, pp. 59-60, 2005.

[141] D. N. Jutla e P. Bodorik, «Sociotechnical architecture for online privacy,» *IEEE Security & Privacy,* vol. 3, n. 2, pp. 29-39, 2005.

[142] S. Pearson , «Taking account of privacy when designing cloud computing services,» in *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing* , Vancouver, Canada, 2009.

[143] M. C. Tschantz e J. M. Wing , «Formal Methods for Privacy,» in *FM 2009: Formal Methods - Second World Congress, Eindhoven, The Netherlands, November 2-6, 2009. Proceedings*, Springer Berlin Heidelberg, 2009, pp. 1-15.

[144] M. Kost, J.-C. Freytag, F. Kargl e A. Kung, «Privacy Verification Using Ontologies,» in *Proceedings of the 6th International Conference onAvailability, Reliability and Security (ARES)*, Vienna, Austria, 2011.

[145] A. Kung, J.-C. Freytag e F. Kargl, «Privacy-by-design in ITS applications: The Way Forward,» in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Lucca, Italy, 2011.

[146] Organization for the Advancement of Structured Information Standards (OASIS), «OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC,» [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se. [Consultato il giorno 4 August 2015].

[147] H. Xu, R. E. Crossler e F. Bélanger, «A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers,» *Decision Support Systems,* vol. 54, n. 1, p. 424–433, 2012.

[148] S. Gürses , «Can You Engineer Privacy?,» *Communications of the ACM,* vol. 57, n. 8, pp. 20-23, 2014.

[149] A. Kung, «PEARs: Privacy Enhancing ARchitectures,» in *Privacy Technologies and Policy: Second Annual Privacy Forum, APF 2014, Athens, Greece, May 20-21, 2014. Proceedings*, Springer International Publishing, 2014, pp. 18-29.

[150] Y.-S. Martín, J. M. del Alamo e J. C. Yelmo, «Engineering Privacy Requirements: Valuable Lessons from Another Realm,» in *IEEE 1st Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*, Karlskrona, 2014.

[151] R. Hörbe e W. Hötzendorfer, «Privacy by Design in Federated Identity Management,» in *IEEE Security and Privacy Workshops (SPW)*, San Jose, California, USA, 2015.

[152] T. J. Karol, «Cross-Border Privacy Impact Assessments: An Introduction,» *ISACA Journal,* vol. 3, 2001.

[153] International Organization for Standardization (ISO), «ISO 22307:2008: Financial services -- Privacy impact assessment,» 1 May 2008. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40897. [Consultato il giorno 21 August 2015].

[154] J. Sun e S. Lee, «A Study on the Implementation of the Effective Privacy Impact Assessment Management System,» in *International Conference on Information Science and Applications (ICISA)*, Suwon, 2013 .

[155] International Organization for Standardization (ISO), «ISO/IEC CD 29134: Privacy impact assessment -- Methodology (Status: Under Development),» [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289. [Consultato il giorno 21 August 2015].

[156] S. Lederer, J. I. Hong, A. K. Dey e J. A. Landay, «Personal privacy through understanding and action: five pitfalls for designers,» *Personal and Ubiquitous Computing,* vol. 8, n. 6, pp. 440-454, 2004.

[157] C. Kuner, «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law,» *Bloomberg BNA Privacy and Security Law Report ,* pp. 1-15 , 2012.

[158] Z. Miners, «Nest, Amazon and their IoT ilk spark privacy concerns,» *CIO,* 11 July 2015.

[159] S. Mason, «The internet and privacy: some considerations,» *Computer and Telecommunications Law Review,* vol. 21, n. 3, pp. 68-84, 2015.

[160] D. Goodin, «Wi-Fi passwords can be stolen by hacking smart lightbulbs,» *Wired,* 8 July 2014.

[161] A. Hern, «Infidelity site Ashley Madison hacked as attackers demand total shutdown,» *The Guardian (Online),* 20 July 2015.

[162] D. Guinard, «Internet of things: businesses must overcome data and privacy hurdles,» *The Guardian (Online),* 1 June 2015.

[163] B. Wasik, «In the Programmable World, All Our Objects Will Act as One,» *Wired,* 14 May 2013.

[164] F. Terpan, «Soft law in the European Union – the changing nature of EU law,» *European Law Journal,* vol. 21, n. 1, pp. 68-96, 2015.

[165] B. Van Vooren, «A case-study of "soft law" in EU external relations: the European Neighbourhood Policy,» *European Law Review,* vol. 34, n. 5, pp. 696-719, 2009.

[166] L. Blutman, «In the trap of a legal metaphor: international soft law,» *International & Comparative Law Quarterly,* vol. 59, n. 3, pp. 605-624, 2010.

[167] C. Pencarrick Hertzman, N. Meagher e K. M. McGrail, «Privacy by design at Population Data BC: a case study describing the technical, administrative and physical controls for privacy-sensitive secondary use of personal informaton for research in the public interest,» *Journal of American Medical Informatics,* vol. 20, n. 1, pp. 25-28, 2012.

[168] N. Graham, «Data protection and privacy,» *Compliance Officer Bulletin,* vol. 98, n. Aug, pp. 1-26, 2012.

[169] M. Kuschewsky, «Sweeping reform for EU data protection,» *European Lawyer,* vol. 112, pp. 12-14, 2012.

[170] D. Hinton-Beales, «Data protection: European parliament, council and commission to begin talks,» *The Parliament Magazine,* 15 June 2015.

[171] R. H. Weber, «Internet of things – new security and privacy challenges,» *Computer Law and Security Review,,* vol. 26, n. 1, pp. 23-30, 2010.

[172] J. Bradley, J. Loucks, J. Macaulay e A. Noronha, «Internet of Everything (IoE) Value Index: How Much Value Are Private-Sector Firms Capturing from IoE in 2013?,» Cisco White Paper 2013. [Online]. Available: http://ioeassessment.cisco.com/learn/2013-ioe-value-index-whitepaper?_ga=1.77770391.2041123141.1433410713. [Consultato il giorno 5 August 2015].

[173] UK Government Legislation, «The draft Microchipping of Dogs (England) Regulations 2015,» [Online]. Available: http://www.legislation.gov.uk/ukdsi/2015/9780111125243. [Consultato il giorno 5 August 2015].

[174] International Organization for Standardization (ISO), «ISO 11784:1996 Radio frequency identification of animals -- Code structure,» 15 August 1996. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=25881. [Consultato il giorno 5 August 2015].

[175] International Organization of Standardization (ISO), «ISO 11785:1996 Radio frequency identification of animals -- Technical concept,» 10 October 1996. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=19982. [Consultato il giorno 5 August 2015].

[176] E. Hupkes, «Regulation, self-regulation or co-regulation?,» *Journal of Business Law,* vol. 5, pp. 427-446, 2009.

[177] Queen Mary, University of London (QMUL), «QMUL Cloud Legal Project,» [Online]. Available: http://www.cloudlegal.ccls.qmul.ac.uk/. [Consultato il giorno 6 August 2015].

[178] Internet Society, «Future Scenarios,» [Online]. Available: http://www.internetsociety.org/internet/how-its-evolving/future-scenarios. [Consultato il giorno 6 August 2015].

[179] D. Papadimitriou (ed.), «Future Internet: The Cross-ETP Vision Document,» 8 January 2009. [Online]. Available: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.future-internet.eu%2Ffileadmin%2Fdocuments%2Freports%2FCross-ETPs_FI_Vision_Document_v1_0.pdf&ei=YARSVcbnIu3B7Aay-YCwBA&usg=AFQjCNGfzMliWHPA0eqvGjMv7qGoY13. [Consultato il giorno 6 August 2015].

[180] N. A. Kazia, «An overview of cloud computing and its legal implications in India,» *Computer and Telecommunications Law Review,* vol. 18, n. 2, pp. 47-53, 2012.

[181] A report by the UK Government Chief Scientific Advisor, Sir Mark Walport, on the internet of things, «The internet of things: making the most of the second digital revolution,» The Government Office for Science, Ref: GS/14/1230, 2014.

[182] S. D. Warren e L. D. Brandeis, «The Right to Privacy,» *Harvard Law Review,* vol. 4, n. 5, 1890.

[183] K. Steinmetz, «These Companies Have the Best (And Worst) Privacy Policies,» *TIME,* 6 August 2015.

[184] D. Hyde e V. Ward, «Samsung SmartTV customers warned personal conversations may be recorded,» *The Telegraph (Online),* 9 February 2015.

[185] P. Spence, «Carphone Warehouse hackers gain access to millions of customer bank details,» *The Telegraph (Online),* 8 August 2015.

[186] Z.-K. Zhang, M. C. Y. Cho e S. Shieh, «Emerging Security Threats and Countermeasures in IoT,» in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Singapore, 2015.

[187] A. Froehlich , «The looming IoT Backlash,» *Network Computing,* 10 June 2014.

[188] Information Commissioner's Office (ICO), [Online]. Available: https://ico.org.uk/. [Consultato il giorno 11 August 2015].

[189] Information Commissioner's Office (ICO), «Register of Data Controllers,» [Online]. Available: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/. [Consultato il giorno 11 August 2015].

[190] J. Fioretti, «EU privacy reform: who pays when the rules are broken?,» *Reuters (Online),* 15 June 2015.

[191] J. Crown, «PM+: One-time consent on data protection rules a 'necessity' for European health research,» *The Parliament Magazine (Online),* 13 March 2015.

[192] T. Kirkhope, «EU data protection measures cannot burden business,» *The Parliament Magazine (Online),* 4 March 2015.

[193] P. Given, «Monetary penalties - lessons learned,» *Privacy & Data Protection,* vol. 12, n. 8, pp. 6-9, 2012.

[194] C. Davies, «Editorial: Data, data everywhere and not a (proper) law in sight,» *Communications Law,* vol. 18, n. 2, pp. 35-36, 2013.

[195] European Data Protection Supervisor (EDPS), «EU Data Protection Reform: EDPS Mobile App,» July 2015. [Online]. Available:

https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package. [Consultato il giorno 17 August 2015].

[196] R. Thomas, «Risk, accountability, and binding corporate codes: a "smarter" approach to data protection,» *Privacy & Data Protection,* vol. 13, n. 7, pp. 3-6., 2013.

[197] European Commission (EC), «Memo: Progress on EU data protection reform now irreversible following European Parliament vote,» 12 March 2014. [Online]. Available: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm. [Consultato il giorno 17 August 2015].

[198] A. Cavoukian, «Letters to the Editor: Operationalizing privacy by design,» *Communications of the ACM,* vol. 55, n. 9, p. 7, 2012.

[199] A. Cavoukian e K. Kursawe, «Implementing Privacy by Design: The smart meter case,» in *Proceedings of the IEEE International Conference on Smart Grid Engineering (SGE),* Oshawa, Ontario, Canada, 2012.

[200] M. B. Islam e R. Iannella, «Privacy by Design: Does it matter for social networks?,» in *IFIP Summer School 2011, International Federation for Information Processing, University of Trento, Trento, Italy.*, 2011.

[201] M. van Lieshout, M. Friedewald, D. Wright e S. Gutwirth, «Reconciling privacy and security,» *Innovation: The European Journal of Social Science Research,* vol. 26, n. 1-2, pp. 119-132, 2013.

[202] A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke e C. Oppenheim, «Privacy Impact Assessments: International experience as a basis for UK Guidance,» *Computer Law & Security Review,* vol. 24, n. 3, p. 233–242, 2008.

[203] R. E. Leenes, «Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology,» *Legisprudence,* vol. 5, n. 2, pp. 143-169, 2011 (Available through SSRN).

[204] R. Brownsword, «Code, control, and choice: why East is East and West is West,» *Legal Studies,* vol. 25, n. 1, p. 1–21, 2005.

[205] N. Robinson, H. Graux, M. Botterman e L. Valeri, «Review of the European Data Protection Directive,» RAND Europe: Technical Report Sponsored by the Information Commissioner's Office (ICO), Cambridge, 2009.

[206] European Privacy Seal: EuroPriSe, «European Privacy Seal for ixquick.com - de-080001p,» 13 July 2008. [Online]. Available: https://www.european-privacy-seal.eu/EPS-en/ixquick. [Consultato il giorno 19 August 2015].

[207] European Privacy Seal: EuroPriSe, «Register of Awarded Seals,» [Online]. Available: https://www.european-privacy-seal.eu/EPS-en/Awarded-seals. [Consultato il giorno 19 August 2015].

[208] J. J. Vanto, «EuroPriSe - the New European Privacy Certification,» *International Association of Privacy Professionals (IAPP),* 1 November 2009.

[209] P. Balboni, Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers, The Hague: T.M.C Asser Press, 2009.

[210] Sheffield Assay Office, «Hallmarking: The Oldest Form of Consumer Protection - A Brief History,» [Online]. Available: http://www.assayoffice.co.uk/our-services/hallmarking. [Consultato il giorno 18 August 2015].

[211] British Standards Institute (BSI), «Product Certification: BSI Kitemark™,» 2015. [Online]. Available: http://www.bsigroup.com/en-GB/our-services/product-certification/kitemark/. [Consultato il giorno 18 August 2015].

[212] Ecolabel Index, Big Room Inc., 2015. [Online]. Available: http://www.ecolabelindex.com. [Consultato il giorno 18 August 2015].

[213] J. Belson, «Ecolabels: ownership, use, and the public interest,» *Journal of Intellectual Property Law & Practice,* vol. 7, n. 2, pp. 96-106, 2012.

[214] T. Mahler, «Defining Legal Risk,» in *Proceedings of the Conference Commercial Contracting For Strategic Advantage - Potentials and Prospects*, Turku University Of Applied Sciences, 2007 (Available through SSRN).

[215] S. Y. Esayas, «Utilizing Security Risk Analysis and Security Testing in the Legal Domain,» in *Risk Assessment and Risk-Driven Testing: First International Workshop, RISK 2013, Held in Conjunction with ICTSS 2013, Istanbul, Turkey, November 12, 2013*, Springer International, 2014, pp. 51-67.

[216] F. Vraalsen , M. S. Lund, T. Mahler , X. Parent e K. Stølen, «Specifying Legal Risk Scenarios using the CORAS Threat Modelling Language,» in *Trust Management: Proceedings of Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005.* , Springer Berlin Heidelberg, 2005, pp. 45-60.

[217] European Commission (EC), «Environmental Assessment,» [Online]. Available: http://ec.europa.eu/environment/eia/home.htm. [Consultato il giorno 17 September 2015].

[218] Privacy Impact Assessment Framework (PIAF) Project, «Home,» [Online]. Available: http://www.piafproject.eu/. [Consultato il giorno 17 September 2015].

[219] European Commission (EC), «Privacy and Data Protection Impact Assessment Framework for RFID Applications,» 2011.

[220] C. Arthur, «DigiNotar SSL certificate hack amounts to cyberwar, says expert,» *The Guardian (Online),* 5 September 2011.

[221] R. Delfino, «European Community legislation and Actions,» *European Review of Contract Law,* vol. 10, n. 2, p. 281–284, 2014.

[222] M. Rosenberg, «And you are...? Will the new Regulation on electronic identification help universities when registering overseas students? Part 1,» *Computer and Telecommunications Law Review,* vol. 21, n. 2, pp. 31-39, 2015.

[223] M. Rosenberg, «And you are...? Will the new Regulation on electronic identification help universities when registering overseas students? Part 2,» *Computer and Telecommunications Law Review,* vol. 21, n. 3, pp. 59-65, 2015.

[224] A. K. Martin e N. N. Gomes de Andrade, «Friending the taxman: On the use of social networking services for government eID in Europe,» *Telecommunications Policy,* vol. 37, n. 9, p. 715–724, 2013.

[225] UK Government, «Guidance: Introducing GOV.UK Verify,» [Online]. Available: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify. [Consultato il giorno 8 October 2015].

[226] Secure idenTity acrOss boRders linKed (STORK) 2.0, «About,» [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=398&Itemid=134. [Consultato il giorno 9 October 2015].

[227] Secure idenTity acrOss boRders linKed (STORK) , «Stork at a glance,» [Online]. Available: https://www.eid-stork.eu/. [Consultato il giorno 9 October 2015].

[228] OPTET Consortium, «D3.4 – Final, consolidated trustworthiness-by-design process, models and tools,» OPTET – 317631, FP7-ICT-2011-8, 2015.

[229] O. C. «D2.4 Socio-economic evaluation of trust and trustworthiness».

7. Annex

(a) Table One: Soft Rule-Making in the Internet Environment

The following list is by no means exhaustive, but offers some examples of the key soft rule-making institutions concentrated on Future Internet themes, such as Internet of Things and cloud technologies, data protection, privacy and security:

Alliance for the Internet of Things (AIOI) [112] was established by the European Commission in 2015 as a forum to join together key stakeholders across a number of sectors and industries. It will assist the European Commission with Internet of Things research, innovation and standardisation policies [113]. The following companies are involved [112]: "Alcatel, Bosch, Cisco, Hildebrand, IBM, Intel, Landis+Gyr, Nokia, ON Semiconductor, Orange, OSRAM, Philips, Samsung, Schneider Electric, Siemens, NXP Semiconductors, STMicroelectronics, Telecom Italia, Telefonica, Telit, Thales, Vodafone, Volvo."

British Standards Institute (BSI) [114] published the British Standard (BS) 10012:2009 for data protection; this includes specification for a personal Information management system. This "provides guidance on putting in place an infrastructure for maintaining and improving compliance with the Data Protection Act."

Body of European Regulators for Electronic Communications (BEREC) [115] – is examining machine-to-machine (M2M) developments.

EuroCloud [116] is a an independent non-profit organisation, which aims to bring together key stakeholders in the cloud services industry, disseminate information, and provide best practice and guidance. EuroCloud operates at two levels: (1) at a national level – EuroCloud has eighteen national components (i.e., EuroCloud UK [117]); and (2) at a European level – EuroCloud Europe acts as a pan-European hub between the members states involved.

European Telecommunications Standards Institute (ETSI) [118, 119, 120] is actively involved with Internet of Things standardisation, through the Connecting Things Cluster and running events to promote discussion on the subject. ETSI is also a founder member [121] of the international oneM2M Partnership Project (see below).

European Union Agency for Network and Information Security (ENISA) provides advice and good practice recommendations for the functioning of the internet market [122].

International Telecommunication Union (ITU) [123] provides a "Global Standards Initiative on Internet of Things (IoT-GSI) promotes a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale". ITU is the United Nations (UN) specialised agency for information and communications technologies [124].

oneM2M [125] is a partnership project that aims to produce cross-sector technical standards for M2M and the Internet of Things.

Online Trust Alliance (OTA) started as an informal industry working group in 2005 to enhance online trust [126]. It is now an international charitable organisation whose members include Microsoft and Symantec. On 11 August 2015, OTA published a draft Internet of Things (IoT) Trust Framework [127], which is aimed at IoT providers. This draft framework proposes twenty-three proposed minimum requirements for any IoT provider self-regulatory or certification programme. It is currently open to industry comment until 14 September 2015. OTA also released its 7th annual Online Trust Audit and Honor Roll [128], which examines the brand protection, security and privacy protection practices of around 1000 websites. In 2015, the top fifty Internet of Things providers were also entered as a new category within this audit.

Organisation for Economic Co-operation and Development (OECD) aims to **"**promote policies that will improve the economic and social well-being of people around the world [129]." This includes the 2013 OECD Privacy Guidelines [130], which propose an internationally agreed set of privacy principles.

Organization for the Advancement of Structured Information Standards (OASIS) [131] administers committees and provides open standards covering a number of areas including: cloud, security, IoT/M2M, privacy/identity and big data.

Perinorm [132, 133] is a bibliographic database containing over 1,400,000 records of national, European and International technical standards and regulations brought together from more than 200 organisations across 23 countries.

UK Anonymisation Network (UKAN) [134] has been set up to provide best practice in anonymisation and practical guidance to anyone managing and sharing personal data. In its first two-years, UKAN is funded by ICO and "co-ordinated by a consortium of four organisations: the University of Manchester, the University of Southampton, the Open Data Institute (ODI) and Office for National Statistics (ONS)."

UK Digital Catapult [135] is working towards improving trust through three key initiatives: (1) convening the Personal Data and Trust Network – "a community that brings together industry, the public sector, funders, research organisations, individual researchers and innovators to support the UK in becoming the global leader in trust and responsible innovation with personal data" [136]; (2) developing the Trust Framework Initiative – "a consumer-centric set of guidelines" [137] concerning the sharing of personal data; and (3) "creating a set of voluntary industry standard icons which consumers can use to make informed decisions about who they trust with their personal data" [135, p. 4].

International Organization for Standardization (ISO) see section 4.3.2.1 for an example.

National regulatory authorities – publish guidance e.g. Information Commissioner's Office (ICO), CNIL France etc.

(b) Table Two: GDPR, Article 23 draft versions

Under Article 23 of the proposed GDPR, data-protection-by-design (DPbyD) would become a legal requirement. The following table displays three versions of draft text from the European Commission [8] on 25 January 2012, the European Parliament [39] on 12 March 2014 and the European Council [40] on 19 December 2014.

Three draft texts	Data Protection Impact Assessment: GDPR Article 33 Draft Text Proposals
	Article 23(1)
European Commission [8]	1. Having regard to the state of the art and the cost of implementation, 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 and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
European Parliament [39] Amendment 129	1. Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, if any, shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular with regard to the principles laid out in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures. 1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to Directive 2004/18/EC of the European Parliament and of the Council 48a as well as according to Directive 2004/17/EC of the European Parliament and of the Council 48b (Utilities Directive). 48a Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (OJ L 134, 30.4.2004, p. 114). 48b Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sector (OJ L 134, 30.4.2004, p. 1).
European Council [40]	1. (…) Having regard to available technology and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.
	Article 23(2)
European Commission [8]	2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
European Parliament [39]	2. The controller shall ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.

European Council [40]	2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary215 for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals. 2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.
Article 23(3)	
European Commission [8]	3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.
European Parliament [39]	-
European Council [40]	(…)
Article 23(4)	
European Commission [8]	4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
European Parliament [39]	-
European Council [40]	(…)

(c) *Table Three: privacy-by-design (PbyD) methodologies*

The following table provides an overview of several significant methodological approaches to PbyD raised by various commentators (however, this is not an exhaustive list; refer to articles for full information):

Year	Author	Brief PbyD Methodological Overview
KEY IDENTIFYING THE MAIN SUBJECT OF THE ARTICLE: **(P) = PbyD Principles (M) = PbyD Model (G) = PbyD Guidelines (S) = PbyD Strategies**		
2001	***Langheinrich*** [138] **(P)**	**Six concepts for optimising privacy within ubiquitous computing** in the order of both technical feasibility and relevance: (1) "notice", (2) "choice and consent", (3) "anonymity and pseudonymity", (4) "proximity and locality", (5) "adequate security" and (6) "access and recourse".
2002	***Yu and Cysneiros*** [139] **(M)**	Demonstrates how the ***i** framework** can be used to model non-functional requirements such as privacy in an agent-orientated context.
2004	***Hong et al.*** [57] **(M)**	The **Privacy Risk Model** split into two parts: (a) **"privacy risk analysis"** – comprised of a number of technological, sociological and organisational privacy questions for design teams to consider during the development process [57, p. 93]; and (b) **"privacy risk management"** – to encourage design teams to rate

		the likelihood, damage and cost of certain privacy breaches as high, medium and low [57, p. 96].
2004	***Lahlou et al.*** [78], [140] (G)	The **European Disappearing Computer Privacy Design Guidelines (Version 1.1)** [78] are aimed at individuals directly involved with software design and development; they encompass nine rules: (1) "think before doing"; (2) "re-visit classic solutions"; (3) "openness"; (4) "privacy razor"; (5) "third party guarantee"; (6) "make risky operations expensive"; (7) "avoid surprise", (8) "consider time"; and (9) "good privacy is not enough".
2005	***Jutla and Bodorik*** [141] (M)	The **Personal Context Agent Networking (Pecan) architecture** is a socio-technical approach to e-privacy; which was developed to: "support users in making informed privacy-related decisions in the presence of uncertainty and across a variety of situations and interacting entities" [141, p. 29].
2009	***Pearson*** [142] (G)	Guidelines for privacy-by-design: (i) "carry out a privacy impact assessment"; (ii) "assess at different phases of design"; (iii) "use privacy-enhancing technologies (PETS) where appropriate"; (iv) ""top six" **recommended privacy practices for cloud system designers, architects, developers and testers** […]: 1. Minimise personal information sent to and stored in the cloud; 2. Protect personal information in the cloud; 3. Maximise user control; 4. Allow user choice; 5. Specify and limit the purpose of data usage; 6. Provide feedback" [142, pp. 47-50].
2009	***Spiekermann and Cranor*** [75] (P) (G)	Identify two interconnected approaches to PbyD: (1) **privacy-by-policy** e.g. the implementation of fair practice principles; and (2) **privacy-by-architecture** e.g. how systems can uphold data minimisation and anonymisation principles.
2009	***Tschantz and Wing*** [143] (S)	Raises the importance of a **formal methods approach** to PbyD i.e. the potential need for "new models, logics, languages, analyses, and tools" relating to privacy [143, p. 8].
2010	***Cavoukian*** [79] (P)	**Seven foundational principles for privacy-by-design**:[71] "1. Proactive not Reactive; Preventative not Remedial […]; 2. Privacy as the Default Setting […]; 3. Privacy Embedded into Design […]; 4. Full Functionality – Positive-Sum, not Zero-Sum […]; 5. End-to-End Security – Full Lifecycle Protection […]; 6. Visibility and Transparency – Keep it Open […]; 7. Respect for User Privacy – Keep it User-Centric […]"
2011	***Gürses et al.*** [77] (P) (S)	Identifies: (1) the **hands-off approach** e.g. vague non-technical definitions and principles of PbyD – "symptomatic of a disconnect between policy makers and engineers"; and (2) the **hands-on approach** e.g. translating PbyD into engineering practice [77, p. 5].
2011	***Kost et al.*** [144] (M)	The **Privacy Assessment Cycle** provides a systematic approach where non-technical privacy requirements identified by key stakeholders are translated by software designers and developers into technical privacy statements. An **ontology-based technical method** is envisioned for the evaluation, formal verification and implementation of the specific privacy requirements raised by the stakeholders.
2011	***Kung et al.*** [145] (P) (M)	The **Impact of Privacy-by-Design on a Process Model** offers a holistic approach by mapping three main PbyD principles – data minimisation, enforcement and transparency – to a generic software design/development process. This model has three stages: (i) privacy requirements (minimisation focus) – requirements and design; (ii) privacy-aware design and implementation

[71] For examples of these seven foundational principles in practice refer to: [167], [198], [199], and [200].

		(enforcement focus) – design and implementation; and, (iii) privacy verification and assurance (transparency focus) – verification and operation.
2011	***van Lieshout et al.*** [55] (P)	**Schematic overview of the privacy-by-design approach based on five building blocks**: (1) "design: guided by privacy principles and values"; (2) "experience of privacy essential for privacy, trust and adoption"; (3) "physical environment: privacy supporting organisation of physical spaces"; (4) "organisation: privacy supporting business processes, management support for privacy"; and (5) "information technology: privacy supporting architecture, privacy enhancing technologies" [55, p. 59].
2012	***Luna et al.*** [80] (M)	**Quantitative threat modelling methodology for privacy-by-design** which incorporates five stages: (1) "define data flow diagrams (DFDs)", (2) "map these DFDs to security and privacy threats", (3) "identify misuse case scenarios", (4) "risk-based quantification of attack tress", and (5) "security and privacy requirements" [80, p. 2].
2012-current	***Organization for the Advancement of Structured Information Standards (OASIS)*** [146] (M)	**OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee** focusing on documentation standards that address privacy governance for software engineers which incorporate the **seven foundational principles for privacy-by-design** [79]***.***
2012	***Xu et al.*** [147] (M)	The **Privacy Enhancing Support System** is a decision support system for privacy protection based on a **value-sensitive design approach**. This application (embedded within a browser) incorporates three privacy-enhancing control tools: (1) PEControl – for controlling personal user data; (2) PESearch – for search; and (3) PEReview – for sharing user ratings a tool "for sharing user ratings and reviews on vendors' privacy practices" [147, p. 424].
2013	***Le Métayer*** [51] (M) (S)	The **Formal Framework for the Analysis of Architectural Choices** integrates the key parameters that impact on the architecture and properties of a system under design, including: (i) service and its purpose, (ii) actors involved and their requirements, and (iii) functionalities of the components available. Also classifies formal models for privacy into three main categories: (i) **language based approaches** e.g. to express privacy policies; (ii) **decentralized security models** e.g. labels to express the confidentiality of a particular dataset; and (iii) **privacy metrics** e.g. measurement of the privacy level pertaining to a particular algorithm.
2014	***Gürses*** [148] (S)	**A small taxonomy of three prominent approaches** to privacy within computer science: (1) **privacy as confidentiality** – a binary understanding of privacy (i.e. the prevention of unwanted disclosures) based on the principles of data minimisation, avoidance of a single point of failure and openness to scrutiny; (2) **privacy as control** – i.e. the creation of practices and mechanisms for compliance with data protection law; and (3) **privacy as practice** – i.e. where individual/collective boundaries of privacy are "negotiated through collective dynamics" [148].
2014	***Hoepman*** [76] (P) (G) (S)	**Eight privacy-by-design strategies** – minimise*, separate*, aggregate*, hide*, inform**, control**, enforce** and demonstrate** – from data protection legislation, OECD guidelines and ISO 29100 privacy principles. Hoepman further builds on [75] by splitting these eight strategies into two categories: (1) **data orientated strategies* (i.e. privacy-by-architecture)** and (2) **process-orientated strategies** (i.e. privacy-by-policy)** [76, p. 452].
2014	***Kung*** [149] (M)	The **Privacy Enhancing Architecture (PEAR) Methodology** is a comprehensive architecture design methodology defined in terms of PbyD, which centres on: (i) quality attributes, (ii) tactics, (iii) PETs, and (iv) risk management.

		It focuses on four tactics categories: (1) minimisation – e.g. anonymous credentials, (2) enforcement – e.g. data protection policies enforcement, (3) accountability – e.g. logging relevant events, and (4) modifiability – e.g. coping with policy changes.
2014	***Martín et al.*** [150] (M) (S)	Explores how **Web accessibility requirements engineering** can be adapted for P/DPbyD; focuses on: (1) principles, (2) guidelines, (3) success criteria, and (4) technique – general or technology-specific.
2014	***van Rest et al.*** [52] (S)	Identify a number of **privacy requirements patterns**, including: "anonimization and pseudonymization"; "hiding of personal data"; "data minimization"; "transparence, auditing and accounting patterns"; and, "informed consent" [52, p. 66].
2015	***Hörbe and Hötzendorfer*** [151] (P) (S)	Focuses on **privacy design requirements**. Identifies **eight privacy and data protection principles** – fairness and lawfulness, finality, proportionality, data quality, information security, openness and transparency, individual participation and accountability – and **architectural requirements** for federated identity management.

(d) *Table Four: GDPR, Article 33 draft versions*

Under Article 33 of the proposed GDPR, data protection impact assessments (DPIAs) would become a legal requirement. The following table displays three versions of draft text from the European Commission [8] on 25 January 2012, the European Parliament [39] on 12 March 2014 and the European Council [40] on 19 December 2014.

Three draft texts	Data Protection Impact Assessment: GDPR Article 33 Draft Text Proposals
Article 33(1)	
European Commission [8]	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
European Parliament [39] Amendment 129	1. Where required pursuant to point (c) of Article 32a(3) the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data. A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.
European Council [40]	1. Where 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 for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller (…)233 shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…). 1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
Article 33(2)	
European Commission [8]	2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

	(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
European Parliament [39]	-
European Council [40]	2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases: (a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions are based that produce legal effects concerning data subjects or severely affect data subjects; (b) processing of special categories of personal data under Article 9(1) (…), biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices (…); (d) (…); (e) (…). 2a. 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 pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board. 2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board. 2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
Article 33(3)	
European Commission [8]	3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, 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.
European Parliament [39] Amendment 129	3. The assessment shall have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall contain at least: (a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation; (d) a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed; (e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned; (f) a general indication of the time limits for erasure of the different categories of data; (g) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented; (h) a list of the recipients or categories of recipients of the personal data; (i) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (j) an assessment of the context of the data processing. 3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding. 3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative shall make the assessment available, on request, to the supervisory authority.

	(The draft also notes that: "Paragraph 3 in the Commission text has partly become points (a), (c), (d) and (e) in Parliament's amendment.")
European Council [40]	3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1, the measures envisaged to address the risk 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. 3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
Article 33(4)	
European Commission [8]	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
European Parliament [39]	-
European Council [40]	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations (…).
Article 33(5)	
European Commission [8]	5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
European Parliament [39]	-
European Council [40]	5. (…) Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
Article 33(6)	
European Commission [8]	6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
European Parliament [39]	-
European Council	6. (…)
Article 33(7)	
European Commission [8]	7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
European Parliament [39]	-
European Council [40]	7. (…)
Other proposed changes	

European Parliament [39] Amendment 128 – Title change [39] Amendment 130 – New article	Change title of Chapter 4, Section 3 from "DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION" to "LIFECYCLE DATA PROTECTION MANAGEMENT".
	Article 33a. Data protection compliance review. 1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment. 2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations. 3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance. 4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative shall make the compliance review available, on request, to the supervisory authority. 5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.

(e) *Table Five: privacy impact assessment (PIA) methodologies*

The following table provides an overview of several significant methodological approaches to PIA raised by various commentators. It further shows the overlap between PbyD and PIA (however, this is not an exhaustive list; refer to articles for full information):

Year	Author	Brief PIA/DPIA Methodological Overview
KEY IDENTIFYING THE MAIN SUBJECT OF THE ARTICLE: **(P) = PIA Principles (M) = PIA Model/Tool (G) = PIA Guidelines**		
1999	***Stewart*** [83] (P) (G)	**Identifies four common elements of PIAs**: (1) "PIA should be **systematic**" e.g. contain a plan of steps to be followed from outset; (2) "PIA should use **competent expertise**" i.e. bringing together experts from number of domains such as technology and law; (3) "PIA should have **independent and public aspects**" i.e. some form of impartial scrutiny; and (4) "PIA to be used in **decision-making**" i.e. "not be divorced from decision-making processes".
2001	***Karol*** [152] (P)	**Offers eight principles for cross-border privacy impact assessments**: (1) "Organizational Responsibility for Ownership of Personally Identifiable Information"; (2) "Identifying the Purpose for which Personally Identifiable Information Is Kept"; (3) "Limiting Data Collection to Business Objectives"; (4) "Required Consent"; (5) "Limitations on the Retention of Personally Identifiable Information"; (6) "Accuracy of Data"; (7) "Data Security"; and, "Training and Communication".
2007 - current	***Information Commissioner's Office (ICO)*** [86] (G)	**Flexible PIA process encompasses seven advised steps**: (1) "identify the need for a PIA"; (2) "describe the information flows"; (3) "identify the privacy and related risks"; (4) "identify and evaluate the privacy solutions"; (5) "sign off and record the pia outcomes"; (6) "integrate the outcomes into the project plan"; and (7) "consult with internal and external stakeholders as needed throughout the process" [86, p. 11].
2008 - current	***International Organization for Standardization (ISO)*** [153] (P) (G)	**ISO 22307:2008: Financial services -- Privacy impact assessment**

2011	***Tancock et al.*** [84] (M)	The **Privacy Impact Assessment Tool for Cloud Computing** (prototype stage) is a decision support system that highlights privacy risks and compliance issues (for jurisdictions currently conducting PIAs e.g. the UK, the US, Australia, New Zealand (NZ), and Canada). It incorporates a knowledge base that is maintained by privacy experts. End users utilise the tool in order to answer a questionnaire from which a privacy impact report is created.
2013	***Sun and Lee*** [154] (M)	The **Privacy Impact Assessment Management System (PIAMS)** is proposed as a support system and process for the creation of PIAs. This process consists of four stages: (1) pre-analysis e.g. establishment of a PIA performance plan, (2) privacy situation analysis e.g. risk assessment, (3) result arrangement e.g. systematic improvement plan in consultation with key stakeholders, and (4) inspection e.g. check performance for each improvement task [154, p. 3].
2014	***Oetzel and Spiekermann*** [59] (M)	Propose **a systematic methodology for privacy impact assessments: a design science approach** comprised of steps: (1) "characterisation of the system"; (2) "definition of privacy targets"; (3) "evaluation of degree of protection demand for each privacy target"; (4) "identification of threats for each privacy target"; (5) "identification and recommendation of controls suited to protect against threats"; (6) "assessment and documentation of residual risks"; and (7) "documentation of PIA process".
2016	***International Organization for Standardization (ISO)*** [155] (P) (G)	**ISO/IEC CD 29134: Privacy impact assessment -- Methodology** is currently under development and expected to be published on 30 November 2016.