BRUSSELS PRIVACY HUB

WORKING PAPER

VOL. 10 • N° 7 • July 2024

Relational Trustworthiness for Cross-Border Data Flows:

On Certification and Model Clauses

By Prof. Sophie Stalla-Bourdillon*

* Co-Director Brussels Privacy Hub, Vrije Universiteit Brussel / Visiting Professor at University of Southampton Law School

DISCLAIMER

The opinions expressed in this paper are those of the author/s.

Contents

Executive Summary

While top-down harmonization efforts, such as those championed through Convention 108+ under the Council of Europe's leadership have made significant strides and should be further strengthened, it is unclear whether these efforts will have sufficient steam to address the multifaceted challenges posed by the emergence of diverse data regimes that are exacerbated by the race to Artificial Intelligence (AI) and diverging approaches towards AI regulation, and whether they are a realistic endeavor beyond a small group of like-minded countries or regions.

Therefore, complementary strategies that embrace bottom-up convergence should be explored to help reduce the divide while trying to avoid triggering a downward spiral. Bottom-up convergence is conceived as the organic alignment of data processing practices through adoption of common standards by stakeholders involved in these practices and operating in or across regions.

The purpose of this paper is to shed light upon the potential of two cross-border data transfer (CBDT) tools that could be used to feed such an organic alignment: standard contractual clauses (SCCs) and certification. Other CBDT tools such as binding corporate rules (BCRs) or codes of conduct have been excluded from the analysis, either because their use case is relatively limited, or because they share similarities with SCCs and certification. SCCs remain the most widely used CBDT tools, while certification is extensively used in industry to produce evidence of compliance with privacy and data protection requirements, including requirements stemming from laws that include CBDT restrictions.

SCCs are model clauses used to form the substance of contractual agreements between data exporters and importers and which establish obligations and safeguards for protecting data during transfer. They essentially act as an extension to data protection agreements or addendums. They usually mirror a pre-existing legal framework, i.e., the framework applicable to the data exporter when it operates domestically, to ensure that minimum standards are exported when the data importer operates in a third country. Certification involves independent assessment of a data importer's data protection practices against predefined criteria or technical standards. These data protection standards and best practices are recognised within the jurisdiction in which the third-party auditor operates, which could be either the data importer's or data exporter's jurisdiction.

This paper compares SCCs and certification through the lenses of a conceptual framework making trustworthiness a key property to evidence in a data transfer context and derives lessons learned from practical implementation of SCCs and certification, including the Cross Border Privacy Rule (CBPR) System and its global extension. It makes the case that certification and SCCs are better viewed as complementary mechanisms and suggests that they should be combined together. Once it is acknowledged that SCCs are simply a subcategory or an extension of DPAs, it becomes harder to argue against their relevance, which does not mean that SCC templates are without criticism. This paper includes five recommendations to improve SCC templates.

Moreover, this paper proposes to clearly distinguish between three assurance levels to accommodate diversity in the CBDT domain and offers a data transfer tool roadmap with five main recommendations to inform the work of policymakers tackling data flows-related challenges. Responding to what seems to be a dominant view in this space, this paper argues that the short-term goal should be to invest in the development of SCCs and the deployment of a modular approach to SCCs based upon substantive requirements (in addition to roles) to facilitate cross-jurisdiction/region comparison and endorsement and more generally ease the identification of the highest common denominator.

Finally, this paper draws some implications in terms of free trade negotiation and global data governance, suggesting that free trade agreements should not treat SCCs differently from certification and that ultimately

building a global data governance forum where a wide range of public policies are confronted is a fundamental next step. It thus cautions against the reduction of the DFFT initiative to the global extension of the CBPR System.

1.Introduction

In the Internet era, data constantly flows across borders. Yet, amidst these ongoing cross-border exchanges, the increasing number of jurisdictions imposing restrictions on data transfers and/or mandating localisation rules has fed the emergence of a patchwork of rules and concerns.[1] These rules stem from varying motivations, including safeguarding human rights, such as rights to privacy and data protection, and asserting data sovereignty. The concept of data sovereignty, in particular, has become a means to address a spectrum of concerns, some of which extend beyond democratic principles. These concerns encompass strategic economic independence, fight or resistance against data monopolies and data imperialism, resilience against cyber threats, and safeguarding national security, among others.[2]

These trends confirms that although globalisation opens up opportunities, it also poses threats to human beings, domestic and global ecosystems often to the detriment of small and medium-size enterprises, provoking a sovereigntist retreat in an increasingly "disoriented" world, as described by Delmas-Marty.[3] It is thus clearly not sufficient to look at the cross-border data transfer (CBDT) domain through oversimplifying pro-growth or innovation-oriented lenses. At the same time, it is becoming increasingly challenging for policymakers and lawmakers to adopt a coherent approach to CBDT, and they are frequently tempted to resort to technological solutionism to evacuate the pondering and the difficult exercise of identifying and addressing underlying trade-offs. Yet, even when Privacy-Enhancing Technologies (PETs) or better Confidentiality-Enhancing Technologies (CETs) are leveraged, trade-offs emerge.[4]

In such a fragmented context, a question arises: how to foster convergences? Although it might appear rather naive in such a highly politicised and militarised context where BigTech and BigStates are so intimately connected,[5] it is crucial to persist in asking this question as data governance challenges are by essence multidimensional and cross-border.

[1] See e.g., N. Cory and L. Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," ITIF Report, 2021, accessed March 12, 2024, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

[2] The European Union often equates data sovereignty with strategic economic independence, while countries from the Global South, such as India, have insisted that data should be used for development. National security is permeating China's approach to cross border data flows, while it is emerging as a key concern in the United States. See T. Christakis, 'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy, 7 December 2020, available at https://ssrn.com/abstract=3748098, accessed 1.5.24; S. Parsheera, Personal Data Protection and Data Transfer Regulation in India, Chapter 2 of the compendium; Li and J. Chen, From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China, 2023, available at https://arxiv.org/abs/2312.08237, accessed 1.5.24, which sheds light on China's "strategic instrumentalisation of the GDPR as a template to shape its unique data protection landscape" and in particular China's cyber sovereignty's agenda. See also Y. Zhang, Personal Data Protection and Data Transfer Regulation in China, Chapter 3 of the compendium; J. Sherman, Biden's Sensitive Data EO Takes an Important Step, 4 March 2024, Lawfare, available at https://www.lawfaremedia.org/article/biden-s-sensitive-data-eo-takes-an-important-step, accessed 1.5.24.

[3] M. Delmas-Marty, Une boussole des possibles - Gouvernance mondiale et humanismes juridiques, Éditions du Collège de France, 2020.

[4] S. Stalla-Bourdillon, Cross-Border Data Transfer Tools vs PETs: a False Debate, Chapter 4 of the compendium.

[5] See A. Mhalla, Technopolitique – Comment la technologie fait de nous des soldats, Seuil, 2023.

While top-down harmonization efforts, such as those championed through Convention 108+[6] under the Council of Europe's leadership have made significant strides and should be further strengthened,[7] it is unclear whether these efforts will have sufficient steam to address the multifaceted challenges posed by the emergence of diverse data regimes that are exacerbated by the race to Artificial Intelligence (AI) and diverging approaches towards AI regulation,[8] and whether they are a realistic endeavor beyond a small group of like-minded countries or regions.

Therefore, complementary strategies that embrace bottom-up convergence should be explored to help reduce the divide while trying to avoid triggering a downward spiral. Bottom-up convergence is conceived as the organic alignment of data processing practices through adoption[9] of common standards by stakeholders involved in these practices and operating in or across regions.[10]

The purpose of this paper is to shed light upon the potential of two CBDT tools that could be used to feed such an organic alignment, i.e., standard contractual clauses (SCCs) and certification, and organise them into a roadmap from which a set of recommendations is derived to inform the work of policymakers involved in global efforts to govern the flow of data across jurisdictions. Other CBDT tools sch as binding corporate rules

[6] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened in Strasbourg, on 10 October 2018 (CETS No. 223).

[7] G. Greenleaf, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108 (October 19, 2011), International Data Privacy Law, Vol. 2, Issue 2, 2012, UNSW Law Research Paper No. 2011-39, Edinburgh School of Law Research Paper No. 2012/12, available at https://ssrn.com/abstract=1960299, accessed 1.5.24; Graham Greenleaf, How far can Convention 108+ 'globalise'? Prospects for Asian accessions, Computer Law & Security Review, Volume 40, 2021. G. Greenleaf has thus recently called for a whitelisting approach including all members to Convention 108+ in Greenleaf, Graham, Dubai's California dreamin': Whitelists for adequacy needed (February 16, 2024). (2024) 187 Privacy Laws & Business International Report 8-13, available at https://ssrn.com/abstract=, accessed 1.5.24.

[8] While the EU has been finalising its Artificial Intelligence Act, which intends to rely upon a risk-based approach without compromising a right-based approach, other jurisdictions have up until now adopted a softer stance. The UK government, in particular, has made it clear that it does not intend to introduce new legislation to maintain a pro-innovation stance. Instead, the Government issued five principles to the UK's regulators in charge of delivering guidance on how these principles will apply to AI systems. See e.g., UK Government, A pro-innovation approach to AI regulation, available at https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary, accessed 11.02.24. It has however been recently mentioned in the press that the UK is currently drafting regulations to govern the most powerful language models. Ellen Milligan, UK Starts Drafting Regulations for Most Powerful Models, Bloomberg, 15 April 2024, available at https://www.bloomberg.com/news/articles/2024-04-15/uk-starts-drafting-ai-regulations-for-most-powerful-models, accessed 1.05.2024. See also President Biden's executive order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence of 30 October 2023, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, accessed 1.5.2024, which sets principles and rules for the federal government and AI deployment and usage. The order is calling for the adoption of a comprehensive privacy law at the federal level. See also state laws such as the Act concerning consumer protections in interactions with artificial intelligence systems adopted on 17 May 2024. On 14 March 2024, the Committee on Artificial Intelligence (CAI) of the Council of Europe approved the draft Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, along with a draft Explanatory Report, available at https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411, accessed 1.5.24.

[9] The adoption can purely voluntary or incentivised, through the express recognition of a range of valid options within the law.

[10] These common standards can be established directly by a regulator (e.g., the European Commission's decision on SCCs), an express request from a regulator addressed to a standard-setting body (e.g., a mandate from the European Commission) or as a result of a bottom-up process led by industry players. See I. Kamara, Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate', in European Journal of Law and Technology, Vol 8, No 1, 2017, who distinguishes between standardisation as collective self-regulation and standardisation as co-regulation.

(BCRs) or codes of conduct have been excluded from the analysis, either because their use case is relatively limited, or because they share similarities with SCCs and certification.[11] SCCs remain the most widely used CBDT tools,[12] while certification is extensively used in industry to produce evidence of compliance with privacy and data protection requirements, including requirements stemming from laws that include CBDT restrictions.[13]

SCCs are model clauses used to form the substance of contractual agreements between data exporters and importers and which establish obligations and safeguards for protecting data during transfer. They essentially act as an extension to data protection agreements or addendums. They usually mirror a pre-existing legal framework, i.e., the framework applicable to the data exporter when it operates domestically, to ensure that minimum standards are exported when the data importer operates in a third country. Certification involves independent assessment of a data importer's data protection practices against predefined criteria or technical standards. These data protection standards and best practices are recognised within the jurisdiction in which the third-party auditor operates, which could be either the data importer's or data exporter's jurisdiction.

The paper is thus structured as follows. Section two compares SCCs and certification through the lenses of a conceptual framework making trustworthiness a key property to evidence in a data transfer context. Section three derives lessons learned from practical implementation of SCCs and certification. Section four proposes a data transfer tool roadmap with some recommendations to inform the work of policymakers tackling data flows-related challenges.

2.Data Transfer Tools through the Lenses of Trustworthiness

After introducing the conceptual framing used to explore the data transfer toolbox centred around the concept of trustworthiness, we compare SCCs and certification along five dimensions to highlight their respective contribution to trustworthiness.

2.1.Conceptual Framing

Although initiatives to promote the interoperability of national data frameworks have framed their goal as fostering trust,[14] it is crucial to differentiate between two closely linked, yet distinct, notions: trust and

[11] Of note, the GDPR has eased the use of BCRs as they can also be used for transfers between different corporate groups engaged in a joint economic activity. GDPR, Article 47(1)(a).

[12] The IAPP-EY Annual Privacy Governance Report 2019 notes that "the most popular of these [transfer] tools – year over year – are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers […]." IAPP-EY Annual Privacy Governance Report 2019, available at https://iapp.org/news/a/2019-iapp-ey-privacy-governance-report-released-at-psr/, accessed 28.11.2023. See also Digital Europe, Schrems II Impact Survey Report, 2020 available at https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf, accessed 28.11.2023, which relies upon a survey conducted between 26 October and 18 November 2020 by DIGITALEUROPE, BusinessEurope, the European Round Table for Industry (ERT) and ACEA following the Schrems II decision in July 2020 ("SCCs are by far the most widely used mechanism for data transfers. Of all companies surveyed, 85 per cent are estimated to use SCCs, while other transfer mechanisms such as adequacy decisions, binding corporate rules (BCRs) or derogations (e.g. consent) account for a little more than 5 per cent of transfers. Only 9 per cent of companies surveyed do not appear to be transferring any data outside the EU.")

[13] This is, for example, the case for certification against the ISO/IEC 27000 family of standards. See Section 3.

[14] See the G20 initiative mentioned for the first time at the G20 OSAKA Summit in 2019 and which is now pursued by the G7 on Data Free Flow with Trust for which Japan has been a strong advocate. See Japan Digital Agency, Data Free Flow with Trust, available at https://www.digital.go.jp/en/dfft-en, accessed 11.2.14. The world economic forum has been a strong advocate of this approach. World Economic Forum, Data Free Flow with Trust – Overcoming Barriers to Cross-

trustworthiness.[15] While trust is an attitude, trustworthiness is a property. Trust is a leap-faith on which to base a decision, it implies accepting risk and vulnerability. Trustworthiness, on the other hand, is a set of qualities considered to be sufficient to elicit reliance. Therefore, it is a means to reduce risk and vulnerability.[16]

The starting point in the context of a commercial relationship is trustworthiness. A party to a commercial relationship relinquishing control over governed data will thus usually require from the other party or other authoritative sources evidence of trustworthiness. Trustworthiness in a cross-border data transfer context can be established at two levels: at the jurisdictional level and/or at the entity level. As a reminder, a data transfer does not necessarily imply data extraction and reallocation of data storage within the environment of the data importer. Mere temporary access by the data importer from a third country to data permanently stored within the jurisdiction of the data exporter is usually enough to characterise a transfer.[17]

Institutional Trustworthiness

When trustworthiness is established at the *jurisdictional* level, it is based upon an institutional analysis of the jurisdiction in which the data importers operate.[18] A one-off institutional analysis may be enough to produce evidence of trustworthiness, although the analysis will need to be reviewed over time. Importantly, a one-off analysis will be relevant for all data importers operating within the jurisdiction under investigation.

Relational Trustworthiness

When trustworthiness is established at the entity level, it is based upon a relational analysis, e.g., an analysis of the commitments and/or behavior of the data importer vis-à-vis the data exporter.[19] A one-off relational

Border Data Flows, White Paper 2023, available at https://www.weforum.org/publications/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows/, accessed 11.2.24.

[15] "To understand, trust, then, we first need to understand the notion of trustworthiness" write P. Smart et al in P. Smart, B. Pickering, B., M. Boniface, & W. Hall, Risk Models of National Identity Systems: A Conceptual Model of Trust and Trustworthiness [Technical Briefing], June 2021, The Alan Turing Institute, available at: https://www.turing.ac.uk/sites/default/files/2021-11/technical_briefing_a_conceptual_model_of_trust_and_trustworthiness.pdf, accessed 1.5.24. See also K. O'Hara, A general definition of trust [Working Paper]. University of Southampton 19pp, 2012, available at: https://eprints.soton.ac.uk/341800/, accessed 1.5.24. Without trustworthiness, trust contributes to risks. R. Ross, M. McEvilley, M. Winstead, Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1, 2022, available at https://doi.org/10.6028/NIST.SP.800-160v1r1, accessed 1.5.24.

[16] There are many conceptualisations of trust (see e.g., A. Etzioni, The moral dimension: Toward a new economics, 1988, New York: Free Press; F. Fukuyama, Trust: Social virtues and the creation of prosperity, 1995, New York: Free Press; C. Lane and R. Bachmann, eds., Trust within and between organizations: Conceptual issues and empirical applications, 1988, Oxford: Oxford University Press). The relationship between contract and trust has long been debated in academia, while the dominant conceptualisation seems to view them as alternatives. See Knights, et al., Chasing shadows: Control, virtuality and the production of trust, 2001, Organization Studies 22/2: 311–336. For the purposes of this policy note, we view contracts as evidence of trustworthiness.

[17] See e.g., EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0., Adopted 14 February 2023, para. 9; EDPB, Data Protection Guide for Small Businesses, available at https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en#toc-4, accessed 1.5.24.

[18] For a conceptualisation of institutional trust see e.g., B.H. Bornstein and A.J. Tomkins, (2015). Institutional Trust: An Introduction, in B.H. Bornstein and A.J. Tomkins (eds), Motivating Cooperation and Compliance with Authority. Nebraska Symposium on Motivation, vol 62. Springer, Cham.

[19] Relational and contractual trust are sometimes distinguished in literature. For the purposes of this paper, we adopt a broad definition of relational trustworthiness, which includes contractual trustworthiness. Relational trustworthiness, just like any form of trustworthiness, sits on a spectrum ranging from weak to strong forms of trustworthiness. As a result, the mere presence of a contract does not necessarily entail that the piece of trustworthiness evidence associated

analysis may be enough to produce evidence of trustworthiness, although ongoing monitoring is crucial to maintain the level of trustworthiness over time. A relational analysis can be performed at two different points in time: either it is performed once and then eventually repeated according to a pre-determined schedule (e.g., once every year) by an independent third party, which means that the same assessment will be supplied to all data exporters with which the certified data importer will interact; or it is performed each time a data importer interacts or contracts with a data exporter, which means it will be repeated at each new interaction.

Burden of Proof

Not all stakeholders are equally equipped to produce evidence of trustworthiness, i.e., produce either an institutional and/or a relational analysis. The burden of proof may thus need to be allocated to a variety of stakeholders, depending upon the type of property to evidence.
Depending upon the regulatory method used for governing cross-border data transfers, at least three options arise:

1. Trustworthiness is established at the entity level, by the parties to the data flow.
2. Trustworthiness is established at the jurisdictional level, by a public authority.
3. Trustworthiness is partially established at the entity and jurisdiction levels, by both the parties to the data flow and a public authority, although each focus upon different properties.

Scaling up the burden of establishing trustworthiness is a preliminary step to reduce the level of complexity of data transfer regimes. It requires making sure that outputs intended to answer the same question are not unnecessarily duplicated, and that the stakeholder that is best placed to produce the output is the official or de facto bearer of the duty. This observation is particularly relevant for evidence of institutional trustworthiness.

In the aftermath of the Schrems II decision, data controllers operating in the European Union (EU) have been asked "to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned." [20] Following its Advocate General, the Court of Justice of the European Union (CJEU) adds that "the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority."[21] One way to refine the EU approach would thus be to scale the burden of establishing trustworthiness by forcing the production of the piece of institutional trustworthiness evidence only once and imposing upon the best-placed stakeholder, i.e., a public body within the jurisdiction of the data exporter, the duty to produce it, or de facto inviting it to produce it. Another way would be to try to avoid inconsistencies of approaches followed for the production of such pieces of evidence.[22] One way to help reduce such inconsistencies would be to adopt a holistic approach to the

with it and which includes it is necessarily strong or weak. See R. K. Woolthuis, B. Hillebrand & B. Nooteboom, Trust, Contract and Relationship Development (2005), Organization Studies, 26(6), 813-840, at 836, who argue that "the contract should be placed in its social context and within the relationship's development."

[20] CJEU Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 16 July 2020, ECLI:EU:C:2020:559 (hereafter Schrems II), para. 142

[21] Schrems II, para. 134.

[22] For example, the European Commission's approach to adequacy decisions has been criticised for following a double standard, e.g., a restrictive standard followed in the EU-US adequacy decision and a more lenient standard followed in other adequacy decisions such as EU-Israel adequacy decision, or EU-Japan adequacy decision or even EU-UK adequacy decision. See EDRI et al, Letter to the attention of Vice-President of the European Commission Věra Jourová, 22 April 2024, available at https://www.statewatch.org/news/2024/april/eu-israel-data-agreement-rings-alarm-bells/, accessed 1.5.24; D. Kouffe, Transfers of personal data from the EU to non-EU countries under the EU General Data Protection Regulation after "Schrems II": not a "Mission Impossible," April 2021, available at https://www.ianbrown.tech/wp-

production of pieces of trustworthiness evidence, which would imply some standardisation efforts to ease the comparison across jurisdictions.

Methods for classifying countries are being used in different sectors. Rubinstein and Margulies, for example, suggest that the EU should adopt a method similar to export control to govern data transfers.[23] Interestingly, President Biden has recently adopted an executive order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern,[24] which as its name suggests, will entail restricting "access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States."[25] Considerations related to human rights are also mentioned, as a justification for setting up such restrictions,[26] which should not lead to generalised data localisation requirements.[27] The OECD declaration of 2022 is used as a benchmark for assessing foreign countries' practices.[28] Such an order will thus lead to the classification of some countries as countries of concern, which is essentially a blacklist approach to cross-border data transfers.[29]

Classifying countries on the basis of rules adopted for granting access to public authorities to data held by private parties does not necessarily imply giving up on the official adequacy assessment, or even moving from a whitelisting approach to a blacklisting approach, if classification only means producing a repository of documented evidence of rules and practices per country and organising them by scope and effect. Such a repository could be produced at the EU level to support the adoption of appropriate safeguards within the meaning of Article 46, and even at the international level, e.g., on the back of the work done by the OECD and the adoption of the non-binding declaration on government access to data held by private sector entities.[30] Making all or part of the research material generated during the negotiation process of the OECD declaration publicly available would be a first step in this direction.

---

content/uploads/2021/04/KORFF-The-EU-regime-on-data-transfers-after-Schrems-II-210422.pdf, accessed 1.5.24. Inconsistencies can also emerge when international commitments undermine the effects of local restrictions. See EDPS, Opinion 3/2024 on the signing and conclusion on behalf of the European Union, of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data, 10 January 2024, available at https://www.edps.europa.eu/system/files/2024-01/24-01-10_opinion_eu-japan_economic_partnership_free_flow_data_en.pdf, accessed 1.5.24, para. 13.

[23] See I. Rubinstein & P. Margulies, Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground 2022(4) Connecticut Law Review 391 ("Borrowing from the graduated structure of U.S. export controls, this Article suggests a graduated model of risk analysis for data transfers.")

[24] Executive order 14117 of 28 February 2024 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern [hereafter EO 14117].

[25] EO 14117, Section 1.

[26] EO 14117, Section 1 ("Such countries' governments may seek to access and use sensitive personal data in a manner that is not in accordance with democratic values, safeguards for privacy, and other human rights and freedoms"). Considerations related to human rights have however also been used to argue for the free flow of data and describe the recent U.S. Trade Representative (USTR) decision to move back from its previous position on data localisation in free trade discussions as digital regression. See Alex Joel, Trusted Cross-Border Data Flows: A National Security Priority, 13 November 2023, Lawfare, available at https://www.lawfaremedia.org/article/trusted-cross-border-data-flows-a-national-security-priority, accessed 28.11.23.

[27] EO 14117, Section 2(g)(ii) ("Any proposed regulations implementing this section: (...) shall not establish generalized data localization requirements to store bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process bulk sensitive personal data or United States Government-related data within the United States").

[28] See EO 14117, Section 1 ("Such countries' approach stands in sharp contrast to the practices of democracies with respect to sensitive personal data and principles reflected in the Organisation for Economic Co-operation and Development Declaration on Government Access to Personal Data Held by Private Sector Entities").

[29] India has recently adopted a blacklist approach to cross border data transfers. See S. Parsheera, n(2).

[30] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487.

Notably, the EDPB has, on its own initiative, contributed to the legal assessment of third countries laws governing access to data by commissioning legal studies on various jurisdictions since 2021. This work could be pursued and extended following the structure of an updated version of the Adequacy Referential [31] and in particular the four essential guarantees: clear, precise and accessible rules for grounding the processing; necessity and proportionality in relation to the objectives pursued by the public authorities when processing the data; independent oversight mechanisms; and effective remedies for individuals. This would not necessarily change the nature of the EDPB's activities, which are grounded on the General Data Protection Regulation (GDPR)[32] Article 70, as the presumption of responsibility would still lie with data exporters, although it would probably require additional resources.[33]

Recommendation:

Consider incentivising competent authorities to make evidence on third countries rules and practices publicly available and eventually refer to relevant institutional trustworthiness metrics including contractual enforceability, enforceability of third party-beneficiary rights, and human-rights standards such as essential guarantees.

Minimum Normative Baseline

A normative baseline is a set of essential principles and intervenability prerogatives aiming at protecting the interests of relevant stakeholders, e.g., the data subject (to whom the data pertain) when the data is personal and/or the end-user of which behavior has been monitored to generate the data, or the data holder.

It is used as a benchmark to assess the trustworthiness of the jurisdiction in which the data importer operates or the date importer itself. When assessing and comparing transfer tools it is thus essential to identify the minimum normative baseline the tool aims to give assurances against. Different normative baselines are used in existing sets of model clauses and certification schemes, e.g., the ASEAN Framework on Personal Data Protection, [34] the APEC Privacy Framework,[35] the Ibero-American Standards for Data Protection,[36] the GDPR, Convention 108[37] and Convention 108+. The ASEAN Framework on Personal Data Protection and the APEC Privacy Framework are both based upon the OECD Guidelines governing the Protection of Privacy and

[31] Article 29 Working Party, Adequacy Referential, WP 254 rev.01.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

[33] The classification would then have to be regularly updated within a pre-determined timeframe defined at the time at which it is first produced. Such a schedule would not eliminate all uncertainties as it is not necessarily possible to anticipate the evolution of domestic laws.

[34] ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin), Framework on Personal Data Protection, available at https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf, accessed 1.5.24.

[35] Asia Pacific Economic Cooperation, APEC Privacy Framework (2015), available at https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1, accessed 28.11.23.

[36] Ibero-American Network on Data Protection, Standards for Personal Data Protection for Ibero-American States, 20 June 2017, available at https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf, accessed 1.5.24. These standards have been developed, taking into account other international standards and in particular "the Guidelines for the Protection of Privacy and the Transboundary Movement of Personal Data of the Organization for Economic Cooperation and Development (OECD); the Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and its Protocol; The Privacy Framework of the Asia-Pacific Economic Cooperation Forum; and the Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and the free movement of such data."

[37] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

Transborder Flows of Personal Data (OECD Privacy Guidelines 2013),[38] which are substantively lower than the GDPR.[39]

As a result, and this is significant, attempting to make transfer tools from different jurisdictions compatible when they reflect significantly different normative baselines will require identifying the highest common denominator.

A normative baseline for cross-border transfer does not have to be identical to or as high, i.e., protective, as the domestic baseline used to protect covered data subjects within a jurisdiction. At the very least, it should capture a set of minimum requirements that a jurisdiction is not willing to compromise on when the data crosses borders, and could therefore very well be interpreted as a set of requirements needed to achieve essential equivalence, as it is the case in the EU.

To avoid double standards and ensure consistency of approaches, the same baseline should be used to assess the trustworthiness of all third countries. In addition, the extraterritorial baseline (i.e., the baseline used to assess the trustworthiness of third countries or data importers operating within third countries) should not be higher, or more protective, than the domestic baseline. However, setting the minimum normative baseline at the right level and clearly communicating it to stakeholders is not necessarily a straightforward exercise, as demonstrated by the debate triggered by the Schrems II decision and the adoption of regulatory guidance to complement such judgment.[40] There are clear evidence that the European Commission (EC) has used a double standard across its adequacy decisions, or that EU Member States benefit from a more lenient standards than third countries.[41]

---

[38] Recommendations of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79. See also ASEAN Framework on Personal Data Protection n(34) ("Having regard to the Asia-Pacific Economic Cooperation forum (APEC) Privacy Framework (2015) as well as other internationally recognised standards or frameworks on personal data protection"); APEC Privacy Framework 2015 n(35) ("The updated Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013)1 with due consideration for the different legal features and context of the APEC region").

[39] See e.g., C. Sullivan, EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era, Computer Law and Security Review, 2019, Volume 35(4), August 2019, p. 380-397 ("Comparison shows that the APEC Framework lacks the particularity, clarity, and guidance required for a standard of this nature; and that it does not generally meet the standard set by GDPR."); See G. Graham, Global CBPRs: A Recipe for Failure?, May 15, 2022, 177 Privacy Laws & Business International Report 11-13, UNSW Law Research Paper No. 22-54, accessed March 12, 2024, available at https://ssrn.com/abstract=4180516, accessed 1.5.24. The APEC Framework already appeared low in comparison to the Data Protection Directive. See G. Greenleaf, APEC's privacy framework sets a new low standard for the Asia-Pacific, in AT. Kenyon, M. Richardson eds, New Dimensions in Privacy Law: International and Comparative Perspectives, Cambridge University Press; 2006, p. 91-120.

[40] The literature is very rich on this topic. See e.g., T. Christakis, ""Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers", European Law Blog, November 2020, Part 1, available at https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-theedpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/, accessed 1.5.24; Part 2: https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2; Part 3: available at https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-postschrems-ii-recommendations-on-international-data-transfers-part-3/, accessed 1.5.24; C. Kuner, Schrems II Re-Examined (VerfBlog, August 25, 2020), available at https://verfassungsblog.de/schrems-ii-re-examined/ accessed 28.11.23; D. Kouffe, n(22); C. Kuner, Article 46, in C. Kuner, L. Bygrave and C. Docksey, The EU General Data Protection Regulation: A Commentary, Update of Selected Articles, Oxford University Press, 2021. See also the 195 comments received by the EDPB after the release of the first version of the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en, accessed 1.5.24.

[41] See e.g., D. Kouffe, n(22); N. Ni Loideain, Brexit, Data Adequacy, and the EU Law Enforcement Directive (February 17, 2022) in Eleni Kosta and Franziska Boehm (eds), The Law Enforcement Directive: A Commentary (Oxford University Press).

2.2.Cross-Tool Comparison

SCCs and certification can be compared along five dimensions. This high-level conceptual comparison reveals that SCCs and certification should be considered as complementary rather than alternative strategies to achieve relational trustworthiness. The benefits of such a complementarity are confirmed by the analysis of a sample of existing schemes in Section 3.

Five Dimensions

Establishment of Trustworthiness

Both SCCS and certification are means to demonstrate relational trustworthiness. SCCs primarily operate at the entity level: they are leveraged to form contractual agreements between data exporters and importers. They focus on specifying a wide range of obligations imposed upon data importers including purpose limitation, data minimisation, downstream control of data usage, warranties for the activities of subcontractors, security and breach notification, accountability and audit, assistance to data exporters, and can also be used to grant third-party beneficiary rights. As a result, SCCs contribute to trustworthiness by formalising contractual obligations between parties involved in a particular data transfer and third-party beneficiaries. With this said, because SCCs can also include to the benefit of data exporters a right to audit or commission a third party to audit data importers' practices, there is potentially an overlap between SCCs and certification.

On the other hand, certification involves assessing in practice the substance of the commitments and behaviour of data importers vis-à-vis data exporters. In other words, it serves as a means to validate trustworthiness through independent assessments of data importers' practices by third parties. By obtaining certification, data importers demonstrate their adherence to established standards once in a particular timeframe.[42] The same certificate is therefore used to evidence relational trustworthiness to all data exporters.

Burden of Proof

The burden of proof typically rests on the data importer entering into a contractual agreement with the data exporter to demonstrate its ability to comply with SCCs. Such a burden of proof is usually fulfilled by exchanging additional documentation based on a non-disclosure agreement, such as answers to privacy and security questionnaires, sharing of internal policies as well as sharing certification or attestation reports during the negotiation process. There is thus an intimate relationship between SCCs and certification.

On the other hand, as regards certification only, the burden of proof primarily lies with the entity receiving the certification vis-à-vis the accredited certification body for which the auditor works to demonstrate its compliance with certification schemes. Auditors conduct assessments to verify adherence to a wide range of established criteria, which usually go beyond due diligence checks performed upon questionnaires and policies as audited organisations usually must demonstrate consistent and effective enforcement of controls addressing threats governed by policies.

Alignment with Minimum Normative Baseline

SCCs aim to align with a minimum normative baseline by incorporating data protection principles and regulatory requirements into contractual obligations. This normative baseline can vary from one set to another.

Certification schemes also include a normative baseline as criteria for assessment. By evaluating data handling practices against this baseline, certification offers assurance that the data importer meets or

[42] See e.g., ISO/IEC TR 17028:2017 Conformity assessment — Guidelines and examples of a certification scheme for services, points 6.8 and 6.9.

exceeds baseline expectations. Once again, the normative baseline can vary from one certification scheme to another.

Minimum Harmonisation Required Across Jurisdictions

There is a fundamental difference between SCCs and certification schemes operated from the jurisdiction of destination, i.e., the jurisdiction of the data importer.[43] While SCCs do require a minimum level of harmonisation across jurisdictions to make sure data importers' obligations and third-party beneficiary rights are enforceable within the jurisdiction of destination, destination-based certification schemes imply a higher level of harmonisation, i.e., the data handling and intervenability standards that are enforceable within the jurisdiction of destination must be comparable with the standards that are enforceable within the jurisdiction of the data exporter, i.e., the jurisdiction of origin. In particular, the list of data subject rights enforceable within the jurisdiction of destination must be comparable with the list of rights enforceable within the jurisdiction of origin.

Effect in Case of Non-Compliance

There are substantial differences between SCCs and certification when non-compliance by the data importer is established.

Non-Compliance with SCCs

Under SCCs, if a data importer fails to comply with the normative baseline outlined in SCCs, this constitutes a breach of contractual obligations and data exporters and data subjects would have legal recourse against the non-compliant data importer based on the terms specified in the SCCs.

Non-Compliance with Certification

Under a certification scheme, when a data importer that has received a certification fails to comply with the normative baseline embedded within the scheme, certification is jeopardized. In practice, once a certification audit has been performed, less intensive surveillance audits are then performed at regular intervals, e.g., every year, until a recertification audit has to be scheduled again, e.g., every three years.[44] When a nonconformance finding is documented by an auditor, the entity has to address it to have a chance to

[43] Note that there is a range of options available for putting in place certification schemes. It is suggested that "[a] safe way to ensure high standards is the accreditation of the local certification body (in the third country) by the national accreditation authority of that country participating in the International Accreditation Forum. I. Kamara et al., Data Protection Certification Mechanisms, Study on Articles 42 and 43 of the Regulation (EU) 2016/679, February 2019, available at https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/04/data_protection_certification_mechanisms_study_final1.pdf, accessed 1.5.14, p. 178.

[44] See e.g., ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, point 9.6.

maintain the certification. Non-conformities[45] may lead to the suspension, reduction in scope[46] or revocation of the certification.[47] This is the case when they are considered to be major nonconformities.

Comparison Upshot

Assuming the goal is to establish relational trustworthiness and reach a high level of assurance, SCCs and certification are best conceived as complementary mechanisms rather than alternatives. This is because they rely upon different approaches to relational trustworthiness. SCCs focus on formalising contractual obligations between data exporters and importers. On the other hand, certification involves independent assessments of an organisation's practices and behaviours to verify compliance with established standards, which may be reflected within the contract binding the data importer to the data importer including the SCCS. These assessments provide additional assurance of the organisation's trustworthiness beyond what is outlined in the contract concluded between the data exporter and the data importer including the SCCs.

The benefits of certification and SCCs are summarised below.

Certification Added Value: Independent and Continuous Validation

While SCCs provide a foundational framework for data transfer relationships by specifying obligations and therefore data protection safeguards, certification offers a more concrete layer of assurance. Certification assessments usually evaluate various aspects of an organisation's data handling and intervenability practices, including data security measures, privacy policies, and compliance procedures. This evaluation provides stakeholders with greater confidence in the reliability and integrity of the organisation that receives the certification, enhancing relational trustworthiness.

In addition, as certification involves third-party validation of an organisation's trustworthiness, it in principle adds credibility and impartiality to the assessment process. This independent validation helps mitigate concerns about self-reporting or bias, providing stakeholders with objective evidence of an organisation's commitment to data protection principles and best practices.[48]

What is more, certification typically involves ongoing monitoring and periodic reassessment to ensure continued compliance with certification standards. This continuous improvement process helps organisations adapt to evolving regulatory requirements and emerging threats, further enhancing their relational trustworthiness over time. In contrast, while SCCs establish initial contractual obligations, they usually do not provide the same level of ongoing oversight and verification as certification.

---

[45] See e.g., ISO/IEC 9001:2005 Quality management systems requirements, point 8.7 ("The organization shall take appropriate action based on the nature of the nonconformity and its effect on the conformity of products and services") and ISO/IEC 19011:2018, Guidelines for auditing management systems, point 6.4.8 ("Nonconformities can be graded depending on the context of the organization and its risks. This grading can be quantitative (e.g. 1 to 5) and qualitative (e.g. minor, major).").

[46] It is important to note that it is not an entity that is certified but a range of processing activities. This means that in some cases, certification may only offer partial assurances. This is true for example when the list of processors in scope for the certification is shorter than the list of processors contracted by the data importer.

[47] This happens on the basis of a legally enforceable agreement concluded between the certification body and its client, as foreseen by e.g., ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, point 5.1. Interestingly, some contracts between data exporters and data importers include an obligation for the data importer to maintain a particular certification during the lifetime of the contract.

[48] Certification bodies are usually required to act impartially. See e.g., ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements, point 6.

SCC Added Value: Rights Enforceability

Although certification is often presented as a technique that is superior to SCCs as certification enables independent and continuous assessment of the data importer's practices as opposed to its commitments, as mentioned above, SCCs can carve out audit rights to the benefit of data exporters and allocate liability between parties.[49]

In addition, SCCs offers one significant benefit that is essential for jurisdictions that have adopted a right-based approach to data protection. While certification provides evidence of an organisation's trustworthiness through independent assessments, SCCs complement this by offering enforceable rights for data exporters[50] and data subjects, and, when annexes are detailed enough, SCCs also offer a window into the data processing practices that are in scope for the data transfer at hand. In the event of non-compliance or data breaches, SCCs provide a legal mechanism for holding the data importer accountable and seeking remedies. This additional layer of enforceability enhances the overall effectiveness of data protection mechanisms in cross-border data transfers and is essential to enable a right-based approach to data protection.

What is more, when SCCs are used to grant third-party beneficiary rights, they can include transparency obligations to the benefit of data subjects.

3.Data-Transfer Tools in Practice

In order to issue insightful recommendations on data transfer tools, it is imperative to go beyond the conceptual framing and comparison performed in Section 2 and comprehend their implementation in practice. Thus, in this section we draw some lessons learned from existing certification schemes and SCCs and consider relevant trends in data and model architectures and AI ecosystems to confirm the importance of certification and model clauses.

3.1.Certification in Practice

The Cross Border Privacy Rules (CBPR) System and its Global Extension

Overview

The Cross-Border Privacy Rule (CBPR) System is a voluntary inter-governmental framework developed by the Asia-Pacific Economic Cooperation (APEC) forum to facilitate cross-border data flows while ensuring a pre-determined level of personal information protection is achieved. [51] The CBPR System is based upon a non-binding principle of mutual recognition: each APEC member is invited to recognise that the level of personal information protection ensured by other participating APEC members is adequate.

Key features of the CBPR System include:

- Principles-based approach: The CBPR System is built on a set of privacy principles derived from the APEC Privacy Framework 2015 and the 2013 OECD Privacy Guidelines. The CBPR System comprises a set of 50 Program Requirements that operationalise the nine privacy principles set forth in the APEC Privacy Framework.[52]
- Voluntary participation: Participation in the CBPR System is voluntary for both APEC member economies and businesses. Companies that choose to participate commit to implementing

[49] See also I. Kamara et al., n(43), p. 198 ff, who stress the importance of binding commitments even when certification schemes are set up.

[50] Data exporters should therefore seriously consider making the obtention and the maintenance of certification a contractual obligation.

[51] The CBPR System builds upon the 2005 APEC Privacy Framework, which was updated in 2015, and comprises nine Privacy Principles.

[52] The intake questionnaire is available at https://privacy.gov.ph/wp-content/uploads/2022/04/Cross-Border-Privacy-Rules-Intake-Questionnaire.pdf, accessed 1.5.24.

and adhering to the CBPR System's privacy principles, while governments agree to support and facilitate the implementation of the framework within their jurisdictions.

- Certification process: Organisations seeking certification under the CBPR System undergo an assessment of their data protection practices by an independent third-party certification body (accountability agent) in their home country. This assessment evaluates the organisation's compliance with the CBPR System's principles.
- Mutual recognition: Once certification is received, participating companies benefit from mutual recognition of their data protection practices across APEC member economies.

Overall, the CBPR System includes two main pillars: a harmonised normative baseline covering data handling obligations and individual rights, plus domestic certification schemes. The Privacy Recognition for Processors (PRP) is an extension to CBPR certification and is specifically designed for data processors.[53] The PRP has fewer Program Requirements than CBPR certification.[54]

The following economies participate in the APEC CBPR System: USA, Mexico, Canada, Japan, the Republic of Korea, Singapore, Australia, Chinese Taipei, and the Philippines. Once an economy joins the CBPR System, it must implement it. Accountability agents have been approved in the United States, Japan, South Korea, Singapore and Chinese Taipei.[55]

At the initiative of the Global CBPR Forum, work is ongoing to transform the CBPR System into a global CBPR framework including both the Global Cross Border Privacy Rules (CBPRs) and the Privacy Recognition for Processors (PRP) System.[56] The System documents have been recently published,[57] and include program requirements based upon the Global CBPR principles.[58] Accountability agents are tasked with examining applicant organisations' intake questionnaires and supporting documentation to verify compliance with the requirements of the Global CBPR System and, assisting the applicants if modifications are required.

Critical Assessment

The CBPR System and its global extension have the merits of highlighting the importance of relational trustworthiness. It is an attempt to build an alternative to the EU adequacy processes, which is by definition focused upon the production of evidence of institutional trustworthiness. The CBPR System and its global extension are based upon the idea that "[b]aseline data protection standards across jurisdictions can be interoperable without being equivalent."[59] Yet, the added value of the concept of interoperability is not clear as it seems to simply imply that a relatively low normative baseline should be sufficient to enable the free flow of data across borders.[60]

---

[53] https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf, accessed 1.5.24.

[54] The intake questionnaire is available here https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf, accessed 1.5.24.

[55] The list of organisations that have received the certification can be found at https://cbprs.org/compliance-directory/cbpr-system/, accessed 1.5.24. They are mainly US based. Within the list, one finds: Apple Inc., Box Inc., HP Inc., Alibaba Cloud (Singapore) Private Limited, Salesforce Inc., …

[56] The 2022 Global CBPR Declaration established the Global CBPR Forum, which seeks to "support the free flow of data by providing an interoperable mechanism for effective data protection and privacy globally." See https://www.globalcbpr.org/, accessed 1.5.25.

[57] https://www.globalcbpr.org/documents/, accessed 1.5.25.

[58] There are two sets of program requirements: one dedicated for controllers and one for processors.

[59] C. Zweifel-Keegan, A globalized CBPR framework: Peering into the future of data transfers, 23 Nov. 2021, IAPP blog, available at https://iapp.org/news/a/a-globalized-cbpr-framework-peering-into-the-future-of-data-transfers/, accessed 1.5.24.

[60] The OECD distinguishes interoperability from harmonisation and proposes the following definition: "ability of different privacy and data protection regimes, or legal frameworks, to work together at multiple levels through policy and practical arrangements and thereby bridge any differences in approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data." L. Robinson, K. Kizawa and E. Ronchi, Interoperability of privacy and data

The normative baseline underlying the CBPR System has indeed been rightly criticised for being much lower in comparison to the standards set forth in the GDPR.[61] While the CBPR System incorporates key data protection principles such as transparency, choice, data integrity, security, and accountability, the requirements are not as stringent or comprehensive as those under the GDPR. For example, the CBPR System does not impose strict requirements regarding data minimisation, storage limitation, or the rights of data subjects, compared with the GDPR.

In addition, enforcement mechanisms under the CBPR System vary depending on the participating APEC member and is not as stringent as those under the GDPR. While companies that receive certification may be subject to audits and assessments by independent third-party certification bodies, there is no centralised enforcement authority or regulatory oversight.[62] What is more, the intention behind the scheme is that most complaints will be resolved by the Accountability Agent's dispute resolution service. More specifically, the model followed by the US with the accreditation of TRUSTe as an accountability agent has been criticised for "[t]he TRUSTe model, in association with an enforcement arrangement based on Trade practices law rather than mandatory privacy principles, means that compliance with the CBPR System in the US will essentially rely on self-assessment, with minimal pro-active oversight or independent checks."[63]

What is more, and this is an important limitation, under the System documents, accountability agents are simply asked to take as input documents produced by applicants.[64] "In-person or phone interviews, inspection of the personal data system, website scans, or automated security tools" are only optional.[65] It would thus be very hard for an accountability agent performing the auditing function to assess alignment and both internal and public-facing policies adopted by an applicant and actual practices. As a result, it is not clear whether a CBPR certification is superior to the combination of other existing certifications and SCCs. It

protection frameworks, Going Digital Toolkit Note, 2012, No. 21, available at https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf, accessed 1.5.24. p. 11.

[61] See G. Graham, n(39); C. Sullivan, n(39); See also Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Recital 79 (The European Commission in its adequacy decision concerning Japan states that in the CBPR System "the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules"). See also I. Kamara et al., n(43), p. 5, ("the actual relationship of the normative criteria and redress mechanisms of such certifications [i.e., CBPR] does not fully correspond to the conditions of the data protection certification mechanisms as provided in Art. 42 and 43 GDPR").

[62] Cooperation of privacy enforcement authorities in the Asia-Pacific region is encouraged through the Cross-border Privacy Enforcement Arrangement (CPEA), which is a multilateral arrangement to facilitate such cooperation.

[63] N. Waters, The APEC Cross Border Privacy Rules system: A Civil Society perspective, June 2013, available at https://privacy.org.nz/assets/Files/International-APPA-APEC/CBPR-Enforcement-Nigel-Waters.pdf, accessed 1.5.25.

[64] "Accountability Agents are responsible for receiving an Applicant Organization's completed Intake Questionnaire and supporting documentation, verifying an Applicant Organization's compliance with the requirements of the Global CBPR System and, where appropriate, assisting the Applicant Organization in modifying its policies and practices to meet the requirements of the Global CBPR System." Global Cross-Border Privacy Rules (CBPR) System Program Requirements Map, available at https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-System-Program-Requirements-Map_Final.pdf, accessed 1.5.24, p.1. See also 5 See accreditation requirements for becoming an APEC CBPR System Accountability Agent available at https://cbprs.org/accountability-agents/cbprs-requirements/, accessed 1.5.24.

[65] The Global CBPR Forum Accountability Agent Recognition Application in this sense mirrors the CBPR System Accountability Recognition Application and states that "[the certification process includes: a. An initial assessment of compliance, which will include verifying the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Applicant Organization against the Program Requirements, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools." See https://www.globalcbpr.org/wp-content/uploads/Accountability-Agent-Application_Final.pdf and https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.pdf, accessed 1.5.24.

should be reminded that certification represent a significant cost for organisations who in practice will necessarily be selective.

Other Certification Schemes

Overview

There are a variety of certification schemes in place already.[66] Although they are not data-transfer specific, they include requirements that are relevant for demonstrating compliance with data transfer restrictions stemming from a variety of legal frameworks including privacy and data protection laws. Here are a few examples.

ISO/IEC 27000 Family

ISO/IEC 27001[67] is s an international standard for information security management systems (ISMS). It includes requirements for establishing, implementing, maintaining, and continually improving an ISMS. Certification to ISO 27001 demonstrates that an organisation has implemented comprehensive security measures to protect its information assets.

Organisations seeking ISO 27001 certification typically undergo an audit by an accredited certification body. The ISO/IEC 27001 certification process comprises a two-stage external audit governed by ISO/IEC 17021-1[68] and ISO/IEC 27006[69] standards: stage 1 consists in "obtaining documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001,"[70] and stage 2 consists in "evaluating the effective implementation of the ISMS"[71] and "to confirm that the client adheres to its own policies, objectives and procedures."[72] What is important to note is that the auditor is charged with assessing the "implementation of controls (…) taking into account the external and internal context and related risks, and the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls declared as being implemented **are actually implemented and effective as a whole**."[73] It is therefore intended to be much more than an assessment of documentation produced by a compliance team.

ISO/IEC 27002[74] complements ISO/IEC 27001 by offering best practices and control objectives related to key cybersecurity aspects including classification of information, access control, identity management, cryptography, and incident response. It is this detailed description of controls that makes ISO/IEC 27002 a particularly rich resource for organisations interested in strengthening their security postures.

ISO/IEC 27701[75] is an extension to ISO 27001, targeting privacy information management systems (PIMS). It includes requirements for implementing, maintaining, and continually improving a PIMS, with a specific emphasis on protecting personal data in the light of applicable privacy or data protection regulations.

Like ISO 27001, the certification process for ISO 27701 involves an audit conducted by an accredited certification body. Organisations are evaluated on their implementation of privacy controls in relation to the role they perform, i.e., controller or processor. Once again, actual implementation and effectiveness of controls is key.

---

[66] For a classification of certification models on the basis of a variety of dimensions see I. Kamara et al., n(43), p. 46 ff.
[67] https://www.iso.org/standard/27001, accessed 1.5.24.
[68] https://www.iso.org/standard/61651.html, accessed 1.5.24.
[69] https://www.iso.org/standard/82908.html, accessed 1.5.24.
[70] ISO/IEC 27006: 2024, para. 9.3.2.1.
[71] ISO/IEC 27006: 2024, para. 9.3.2.2.
[72] ISO/IEC 27006: 2024, para. 9.3.2.2.
[73] ISO/IEC 27006: 2024, para. 9.3.2.2.(f) (emphasis by the author).
[74] https://www.iso.org/standard/75652.html, accessed 1.5.24.
[75] https://www.iso.org/standard/71670.html, accessed 1.5.24.

SOC 2

SOC 2[76] is a framework developed by the American Institute of Certified Professional Accountants (AICPA) for assessing data handling practices based upon five principles or trust service criteria:[77] security, availability, processing integrity, confidentiality, and privacy. It is commonly used by technology companies, particularly those offering cloud services or Software-as-a-Service solutions, to demonstrate their commitment to protecting customer data.

Organisations undergo an independent audit by a certified public accountant (CPA) to assess their controls against the criteria defined in the SOC 2 framework. The audit evaluates the effectiveness of security and privacy controls in place, focusing on areas such as data protection, system monitoring, and incident response. Although ISO/IEC 27001 and 27701 certification is more comprehensive than SOC 2 attestation, producing a SOC 2 attestation also requires assessing the effective implementation of scoped controls.[78]

EuroPrivacy

EuroPrivacy is different from the standards listed above in that it is not set forth upon industry consensus-based standards but upon hard law requirements, i.e., the GDPR. This said, it is described as being easily combined with ISO/IEC 27001 certification.[79] As evidenced by the GDPR core criteria,[80] which are used as benchmarks to evaluate the applicant's policies and controls, this scheme goes beyond the ISO suite or the SOC 2 attestation process in that it is strictly mapping to GDPR rules. When compliance is dependent upon a legal assessment, these criteria mandate the production of a document or report demonstrating that the legal assessment has been performed by a data protection officer or a legal expert with adequate expertise. Most of the GDPR core criteria include requirements to have rules, policies or processes in place to address a particular GDPR provision or set of provisions.

As regards data transfers, criterion G.10.1.1 B) states the transfer should be assessed as lawful by a DPO or legal expert with adequate expertise. The cross-border data transfer tool should be expressly acknowledged under G.10.1.2, and data transfers should be regularly audited under G.10.1.3. The DPO is also asked to assess and confirm that data subjects can effectively exercise their rights and access legal remedies. Very interestingly, under G.10.1.6., it is required that the data importer make "binding and enforceable commitments to apply appropriate safeguards to protect the processed data with regards to the rights of the data subjects." The importance of contractual commitments mentioned in previous sections is thus confirmed by the EuroPrivacy scheme itself.

Of note, the EDPB's register of certification mechanisms, seals and marks [81] also include four national certification schemes.

EUCC

Under Regulation (EU) 2019/881,[82] the EU cybersecurity certification framework governs the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. The

[76] https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services, accessed 1.5.24.
[77] The 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022) (2017 TSC).
[78] Ibid, para. 16. ("A type 2 SOC 2 engagement, which includes an opinion on the operating effectiveness of controls, also includes a detailed description of tests of controls performed by the service auditor and the results of those tests").
[79] https://www.europrivacy.org/, accessed 1.5.24.
[80] https://community.europrivacy.com/europrivacy-gdpr-core-criteria/, accessed 1.5.24.
[81] https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en, accessed 1.5.24.
[82] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15–69.

European Cybersecurity Scheme on Common Criteria (EUCC) drafted by the European Union Agency for Cybersecurity (ENISA) is the first scheme within the EU cybersecurity certification framework to be adopted.[83] The scheme is based on the SOG-IS Common Criteria evaluation framework already leveraged across a substantial number of EU Member States. It includes two levels of assurance based on the level of risk associated with the intended use of the product, service or process. ENISA is also working on two more cybersecurity certification schemes, EUCS on cloud services and EU5G on 5G security.

Critical Assessment

Overall, these certification schemes offer valuable means for organisations to demonstrate the reality of their commitments to information security, privacy and data protection standards.

However, they present limitations, particularly in terms of the substantive assessment performed by third-party auditors. While the certification process involves comprehensive evaluation of policies and procedures against established standards, alignment of practices and effectiveness of controls, the main criterion for evaluation remains consistency (between policies and practices) and not lawfulness (of practices) under applicable laws. This means that auditors primarily assess whether the organisation's policies are consistently followed in day-to-day operations and data is adequately protected under these policies. The EuroPrivacy scheme stands out, however, in that it has a clear focus upon lawfulness under the GDPR. When legal assessment is needed, it is nonetheless delegated to DPOs or legal experts, and the external auditor's task is then to verify whether a role, with appropriate expertise, has been involved in the assessment.

In other words, auditors typically do not delve into substantive aspects, such as the quality of data classifications or impact assessments, the quality of the information provided to data subjects (beyond its consistency with actual practice) or the quality of the organisation's response to data subject requests. Yet, these substantive aspects remain crucial for claiming data protection and privacy compliance. As a result, certification cannot serve as a mere substitute for data-handling contractual obligations and third-party beneficiary rights, although they are essential assurance mechanisms.

3.2.Standard Contractual Clauses in Practice

SCC Adoption

As mentioned in the introduction, SCCs are the most widely used CBDT tool, at least by data exporters operating in the EEA. This was true before the Schrems II decision and continues to be true after the Schrems II decision. Despite the introduction of new transfer tools within the toolbox of European Economic Area (EEA) Member States and other jurisdictions[84] that have been influenced by the GDPR standard, it is not surprising to see that, in practice, SCCs regularly complement DPAs, be they incorporated by reference or included within an exhibit to the main DPA, which explains recent efforts to compare model clauses across regions.[85]

This state of play can be explained by at least three reasons.

---

[83] See e.g., https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme, accessed 1.5.24.

[84] E.g., Brazil. Interestingly, although China has clearly been influenced by the GDPR when drafting its own Personal Information Protection Law (PIPL), PIPL transfer tools do not replicate GDPR ones. New transfer tools are introduced, the most prominent of them being a security assessment to be approved by the Cyberspace Administration of China (CAC). On 7 July 2022, the CAC released the Measures for the Security Assessment of Cross-border Data Transfer,[94] which came into effect on 1 September 2022.

[85] See the FPF's work, Lee Matheson, Not-So-Standard Clauses – Examining Three Regional Contractual Frameworks for International Data Transfers 2023, available at https://fpf.org/wp-content/uploads/2023/03/FPF-SCC-Not-So-Standard-Clauses-Report-FINAL-single-pages-1.pdf, accessed 28.11.23; the work of the European Commission itself, which released a joint guide on EU SCCS and ASEAN model clauses. European Commission, Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses available at https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf, accessed 28.11.23.

First, the CJEU has not directly invalidated SCCs, contrary to the EC's adequacy decision setting the foundations for the Privacy Shield Framework.

Second, they require low resources for their adoption and are relatively flexible, as they do not need to be pre-approved before being signed by both parties.

Third, they enable the data exporter to gather a binding commitment directly from the data importer, which is often considered as a must-have in practice, even when there is no concern about the protection of data subjects' fundamental rights. Data exporters who are well-versed in data security practices clearly have an interest in agreeing upon rules limiting the purposes for which the data will be processed, triggering the deletion of the data once the contract is expired or terminated, governing the involvement of third parties into the processing or the downstream data sharing, imposing the notification of actual or suspected incidents impacting the confidentiality, authenticity, integrity, availability of the covered data and stipulating audit rights. In this sense, SCCs should thus be seen as a mere extension of data protection agreements, addendums or data sharing agreements, which often tend to cover more than personal data, even if no applicable law mandates such an extension.[86] This is confirmed by the EC itself, which states in its FAQs that as regards the controller-to-processor module, there is no need to extend it with a DPA: in other words, the SCCs are the DPA.[87] Once SCCs are viewed in this light, they become good candidates for expressing binding commitments in a cross-border data transfer context, and thereby complementing data importers' certifications.

Although this is rarely admitted by parties to a data transfer, or at the very least by their business sponsors, SCCs can have clear benefits for both parties and third-party beneficiaries. This is true, for example, for the EU SCCs, which comprise a descriptive annex that aims to force parties to disclose the cross-border data flows that are in scope for the specified processing purposes and to which data subjects have a right to access.[88] EU SCCs must therefore have had an impact upon the level of transparency surrounding data flows, at least between parties with some bargaining power, although more could be done to transform data subjects' *formal* access rights into *real* access rights.[89]

Of note, even when a jurisdiction chooses not to adopt data transfer restrictions methods, recent privacy and data protection reforms have led to the introduction of an explicit or implicit obligation imposed upon covered entities to conclude a contract with service providers processing data exporters' data, with a view to impose a series of obligations upon the latter, including when they are not covered entities themselves.[90] Therefore, the number of jurisdictions that conceive contracts as regulatory instruments of which function is

[86] It is such an extension that makes contract negotiations more convoluted.

[87] Commission's answer to FAQs 21, available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en, accessed 28.11.23 ("For data transfers from controllers to processors, or processors to sub-processors, the requirements of Article 28 of the GDPR have been incorporated into the SCCs. Companies therefore do not need to sign a separate contract to comply with Article 28 of the GDPR.")

[88] This should not be neglected as data subjects do not have access to recording of processing activities, or data protection impact assessments under the GDPR (see Articles 30 and 35). When filled properly, annexes to SCCs contain however important information about categories of personal data in scope, categories of data subjects to whom the personal data pertain, purposes of data flows by role, processing activities performed by processors and sub-processors, data retention, and technical and organisational measures put in place to protect personal data.

[89] The EU SCCs impose an obligation upon data controllers to share SCCs with data subjects when the latter request access to them (see clause 8.2(C) Module 1, clause 8.3 Module 2 and 3). There has not been a lot of enforcement effort spent on making this requirement a reality, however.

[90] See for example the California Consumer Privacy Act, as amended by the California Consumer Privacy Rights. Cal. Civ. §1798.100. See also Quebec Law 25, which through its transfer impact assessment requirement is essentially implicitly requiring the conclusion of contracts between covered entities and service providers (Section 17(4) of the Act respecting the protection of personal information in the private sector.)

to export privacy and data protection standards could be considered as de facto higher than the number of jurisdictions that have officially adopted transfer restriction rules.

Building a coherent set of model clauses to cover a variety of data flows is however not straightforward, and it is easy to get caught by the intricacies of the laws the model clauses are supposed to reflect. The complexity of the EU model has been rightly criticised: the multi-module approach continues to lead to misunderstandings on the ground,[91] and it is unclear why more than five years after the entry into force of the GDPR we are still waiting for model clauses that should govern transfers to data importers that are subject to the GDPR under Article 3(2).[92] Difficulties increase when an organisation operates at the global level and it has to refer to a variety of sets of model clauses.

Existing Models

There are already several sets of model clauses, which have been developed in various parts of the world.

- EU SCCs

Under the GDPR, SCCs can be used as a ground for data transfers from the EU to third countries. These model clauses are "pre-approved" by the European Commission. On 4 June 2021, the Commission issued a modernised set of clauses comprising four modules to replace the sets that had been adopted under the old Data Protection Directive 95/46.[93]

It is up to the parties to the data transfer to decide whether to use SCCs to legally ground the transfer or not under GDPR Chapter V. If the SCCs are adopted, there is no need to check whether the law of the Member State in which the data exporter operates adds to the requirements covered by the SCCs.

As regards third-party beneficiaries, clause 3 recognises the rights of data subjects to invoke and enforce the SCCs against the data exporter and/or the data importer with some exceptions.[94]

- UK and Switzerland

[91] See e.g., Victoria Hordern, EU standard contractual clauses: the curious case of Module 4 for data transfers, 30 January 2023, available at https://www.taylorwessing.com/en/insights-and-events/insights/2023/01/eu-standard-contractual-clauses, accessed 28.11.23 whom suggests that Module 4 is not fit for purpose.

[92] See Commission's answer to FAQs 24, n(87) (" They do not work for importers whose processing operations are subject to the GDPR pursuant to Article 3, as they would duplicate and, in part, deviate from the obligations that already follow directly from the GDPR. ")

[93] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 7.6.2021, p. 31–61.

[94] Importantly, clause 6, which stipulates that the parties must fill in an annex describing the transfer, is within the list of exceptions.

The UK and Switzerland have endorsed the EU SCCs as a valid transfer mechanism, once completed by an addendum[95] or adapted/supplemented by appropriate information, which is more administrative than substantive in nature.[96]

- Convention 108+ Model Contractual Clauses

These Model Contractual Clauses aim to enable the transfer of personal data to countries that are not parties to Convention 108 as amended by the Protocol CETS No. 223.[97] Only one module is available: the module for controller-to-controller relationships. This module will be complemented with two other modules to be adopted by the Consultative Committee. These Model Contractual Clauses will be further developed or approved by the Convention Committee set up under Chapter VI of Convention 108+, once the Protocol CETS No. 223 amending Convention 108 will enter into force.

These clauses must be approved by each party to the Convention, who will then endorse them as valid standardised contractual tool for data transfers. When approving such clauses, each party will have to assess them in the light of its domestic law and verify that they are compatible with such law.

These model clauses are not necessary for transfers between entities operating in jurisdictions that are parties to the Convention.[98] For transfers to the jurisdiction of a state or international organisation which is not a party to the Convention, parties to the Convention can adopt a range of "ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments,"[99] including model clauses.

As regards, third-party beneficiaries, clause 7 stipulates that data subjects are entitled "to invoke the safeguards and guarantees set out in Section II and III of these Clauses as a Third-Party Beneficiary with respect to any provisions of these Clauses affording a right, action, claim, benefit or privilege to such Data subject." This approach appears to be more limiting that the approach taken by the EU SCCs, as the exercise of third-party beneficiary rights would be dependent upon the demonstration that the clause affords a right, action, claim, benefit or privilege to the data subjects.

- ASEAN Model Contractual Clauses (MCCs)

[95] See Information Commissioner's Office, International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, accessed 1.5.24. The UK has also developed its own set of model clauses. See Information Commissioner's Office, International Data Transfer Agreement, version A1.0, in force 21 March 2022, available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf, accessed 1.5.24.

[96] The Federal Data Protection and Information Commissioner (FDPIC) recognises the EU SCCs, with the caveat that they will be adapted and/or supplemented as necessary in specific cases. FDPIC, The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts, 27 August 2021, available at https://www.edoeb.admin.ch/edoeb/en/home/kurzmeldungen/2021/20210827_datenuebermittlung_ausland.html, accessed 1.5.24. More generally, the FDPIC recognises three sets of clauses: the EU SCCs, the Swiss Transborder Data Flow Agreement (for outsourcing of data processing) of November 2013 and the Council of Europe model contract to ensure equivalent protection in the context of cross-border data flows.

[97] Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Model Contractual Clauses for the Transfer of Personal Data – Module 1, Strasbourg, 16 June 2023, T-PD(2022)1rev10final. The clauses can now be pre-approved by competent national authorities to be included in the official set of transfer mechanisms for data controllers.

[98] Convention 108+, Article 14.

[99] Convention 108+, Article 14(3)(b).

ASEAN is an intergovernmental organisation of ten Southeast Asian countries,[100] who do not share a common and binding normative baseline in the domain of privacy and data protection. The MCCs[101] however embed a baseline derived from the ASEAN Privacy Framework on Personal Data Protection of 2016.[102] Because the laws of ASEAN Member State may be more demanding, private entities are encouraged to verify if the ASEAN Member State in which they operate have issued further guidance or additional templates.

The MCCs are thus a voluntary standard, which might not even have been endorsed by the jurisdictions of the parties to the data transfer.[103] The MCCs have been designed for intra-ASEAN flow of personal data, but private entities using these clauses have the possibilities to adopt these clauses for both transfers between businesses intra-ASEAN, or transfers to non-ASEAN Member States, in particular when third countries have legal regimes based upon the principles of the APEC Privacy Framework or OECD Privacy Guidelines, from which the principles of the ASEAN Framework on Personal Data Protection (2016) are based. Adaptation or amendment are possible provided they do not contradict the MCCs.[104]

The MCCs comprise two modules: one governing controller-to-controller relationships and one governing controller-to-processor relationships. "Their usefulness to SMEs as a low-cost basis for data exports"[105] has been questioned. One important consideration for our purpose stems from the fact that "the ASEAN MCCs give no enforceable rights to data subjects,"[106] although the MCCS offer a set of additional terms for individual remedies when the law designated by the parties recognise third party rights. What this example shows, therefore, is the importance of ensuring the adoption of a minimum normative baseline to make model clauses an effective mechanism for the protection of data subject rights.

- Ibero-American Network Clauses (MTAs)

The Ibero-American Data Protection Network (RIPD, after its acronym in Spanish) is a network of 16 data protection authorities from Ibero-American countries. The members of the RIPD include Mexico, Andorra, Spain, Argentina, Chile, Colombia, Costa Rica, Panama, Peru, Brazil, Uruguay, and Portugal. The Spanish DPA is the network's permanent secretariat.[107]

[100] Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam.

[101] ASEAN Model Contractual Clauses for Cross Border Data Flows, Final Copy Endorsed by the 2nd ASEAN Digital Senior Officials' Meeting (ADGSOM), January 2021, available at https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf, accessed 1.5.24.

[102] See n(34).

[103] Some ASEAN jurisdictions, such as the Republic of the Philippines and Singapore have endorsed the use of these clauses. The Personal Data Protection Commission of Singapore (PDPC) states, for example, that "it recognises and encourages the use of the ASEAN MCCs to fulfil the Transfer Limitation Obligation1 under the Personal Data Protection Act (PDPA)" and what is more that "The ASEAN MCCs can also be used to fulfil the Transfer Limitation Obligation under the PDPA for countries with data protection regimes based on the APEC Privacy Framework or OECD Privacy Guidelines." PDPC, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore, 22 January 2021, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.pdf, accessed 1.5.24.

[104] Ibid, p. 4.

[105] G. Greenleaf, ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards, 2021, 174 Privacy Laws & Business International Report 22-24.

[106] Ibid ("Some of the AMS are common law countries (Malaysia, Brunei, Singapore, and Myanmar to some extent) where part of their inheritance of the common law from the UK included the doctrine of privity of contract, which prevents data subjects from relying on provisions in an exporter-importer contract because they are not a party to it. Statutory provisions do override this in some countries, in some cases, but there must usually be a clear intention in the contract that the data subject must benefit, and that is not obvious from the ASEAN MCCs. A morass of ambiguity and statutory interpretation is not much help to data subjects.") See also G. Greenleaf, Asian Data Privacy Laws (OUP, 2014), p. 500ff.

[107] See https://www.redipd.org/es/la-red/entidades-acreditadas, accessed 1.5.24.

On September 27, 2022, the Ibero-American Data Protection Network (RIPD) released the Guide for Implementing Standard Contractual Clauses for International Personal Data Transfers (the Guide).[108] The document outlines specific considerations for conducting international transfers of personal data using standard contractual clauses (referred to as Model Transfer Agreements - MTAs), guiding entities conducting data transfers from RIPD member countries to importers located in jurisdictions lacking adequate data protection measures[109] or non-adequate countries (according to the regulations of the data exporter's country or the interpretation of the competent data protection authority).

Just like the ASEAN MCCs, the MTAs have been used to embed a normative baseline, i.e., the non-binding normative baseline stemming from the Standards for Personal Data Protection for Ibero-American States.[110]

The RIPD MTAs are described as being compatible in their structure with the 2021 EU SCCs.[111] The Guide proposes two sets of MTAs: one for transfers between controllers and the other for transfers between controllers and processors.[112] These two types are not meant to be final, and the drafting of MTASs templates for processor-to-processor and processor-to-controller is foreseen for the future.[113] As of today, Peru, [114] Uruguay, [115] and Argentina[116] have either approved or issued recommendations regarding RIPD model clauses.

Overall, the Guide aims to help regulators in crafting tools that help entities handling personal data fulfil the requirements of Article 36.1(c) of the RIPD's Standards for Personal Data Protection for Ibero-American States,[117] which allows data transfers via signed contractual clauses or similar instruments, ensuring adequate guarantees.[118] These clauses must provide adequate assurances, demonstrating (i) the extent of personal

[108] Available (in Spanish) at https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf, accessed 1.5.24.

[109] G. C. Munoa, M. A Roth, S. Requejado, J. Manuel, 'Multijurisdiction: Ibero-American Network for the Protection of Personal Data - Standard Contractual Clauses for the International Transfer of Personal Data' (*Global Compliance News*, 23 October 2022), available https://www.globalcompliancenews.com/2022/10/23/multijurisdiction-ibero-american-network-for-the-protection-of-personal-data-standard-contractual-clauses-for-the-internal_10232022/ , accessed 11.4.24.

[110] See n(36). In June 2017, the RIPD published the Standards for Personal Data Protection for Ibero-American States. It sets out common principles and rights for personal data protection that Ibero-American countries can use to create or update their domestic data protection laws. The goal is to have consistent rules across the region.

[111] RIPD, Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales, available at https://www.redipd.org/es/noticias/guia-sobre-transferencias-internacionales-de-datos, accessed 1.4.2024.

[112] 'Argentina's AAIP Endorses Ibero-American Data Protection Network SCCs' available at https://iapp.org/news/a/argentinas-aaip-endorses-ibero-american-data-protection-network-sccs/, accessed 15.4.24.

[113] G. C. Munoa n(109).

[114] Autoridad Nacional de Transparencia y Acceso a la Información Pública, Resolución Directoral N.º 074-2022-JUS/DGTAIPD, 17 October 2022, available at https://cdn.www.gob.pe/uploads/document/file/3787915/RD%20074%20Clausulas%20contractuales%20modelo.pdf.pdf?v=1666656624, accessed 1.5.24.

[115] Unidad Reguladora y de Control de Datos Personales Resolución N° 50/022, 29 December 2022, available at https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022, accessed 1.5.24.

[116] Agencia de Accesso a la Información Pública, Resolución 198/2023, RESOL-2023-198-APN-AAIP, 13 October 2023, available at https://www.boletinoficial.gob.ar/detalleAviso/primera/296189/20231018, accessed 1.5.24.

[117] See n(36).

[118] "36. General Rules for Transferring Personal Data
36.1. The person responsible and the person in charge may perform international transfers of personal data under any of the following assumptions: [...] c. Exporter and recipient sign contractual clauses or any other legal instrument that offers sufficient guarantees and that allows proving the scope of the treatment of the personal data, the obligations and responsibilities assumed by the parties, and holders' rights. The control authority may validate the contractual clauses or legal instruments, as determined in the national legislation on the matter, of the Ibero-American State".

data processing, (ii) the obligations and responsibilities of both parties and (iii) the rights of data subjects. The concerned supervisory authority is authorised to approve contractual clauses under the applicable domestic legislation.

The Guide states that the data subject is a third-party beneficiary in the Transfer Agreement signed by the exporter and importer. This means that the data subject has rights that derive not only from the personal data protection law of the data exporter's jurisdiction but also from the international transfer contract itself. The RIPD MTA "provides blanket authorization for third parties to enforce the clauses against importers and exporters without any exceptions."[119]

Regarding the evaluation of local laws and government/public authorities access requests, RIPD MTA requires parties to assess the laws and practices of the receiving jurisdiction that could affect the compliance of the Model Agreement. In this sense, clause 11 of Module 1 states that Parties must confirm they have made reasonable efforts to identify whether the transferred data are covered by any local law or practice of the jurisdiction of the data importer that goes beyond what is necessary and proportionate in a democratic society to safeguard important objectives of public interest and can reasonably be expected to affect the protections, rights and guarantees granted under the Transfer Agreement to the data subject. Then, the importer should notify the data exporter immediately if any of these laws apply to it in the future.[120]

The MTAs remains a voluntary standard. In the event of a clear contradiction between the MTAs and a local authority's recommendation or guidance, the guide to the MTAs suggests following the recommendation or guidance of the local authority.[121]

Model clauses developed by or in development within single jurisdictions such as Argentina,[122] Uruguay,[123] New-Zealand,[124] Brazil[125] and China[126] should also be mentioned. It is worth noting that although Brazil is a member of the Ibero-American Network, it has not endorsed the MTAs yet.

What the review of existing sets of model clauses show is there seems to be value in developing model clauses, even if the local law does not include them within the list of official CBDT tools. This is of particular relevance when considering data protection frameworks like the recently adopted Indian one, which is relatively open and relies upon a blacklist approach.[127]

---

[119] See Lee Matheson, n(85).

[120] If such notification is made or if the data exporter has reason to believe that the importer can no longer comply with the obligations of the Transfer Agreement, the exporter will identify the appropriate measures to remedy the situation. Likewise, it may suspend the transfers if it considers that adequate guarantees cannot be ensured.

[121] Ibid, p. 3.

[122] Ministerio di Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales, Disposición 60 - E/2016, available at https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm, accessed 1.5.24.

[123] Uruguay, Resolución N° 41/021, de 8 de setiembre de 2021, available at https://www.gub.uy/unidad-reguladoracontrol-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay, accessed 1.5.24.

[124] One way to comply with Information Privacy Principle 12 responsibilities when transferring personal information to a third country is to have model clauses in place. Privacy Commissioner, Agreement for Cross-Border Transfer of Personal Data, available at https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/, accessed 1.5.24.

[125] Autoridade Nacional de Proteção de Dados, Proposal for Regulation on International Transfer of Personal Data, available at https://www.gov.br/participamaisbrasil/regulation-on-international-transfer-of-personal-data, accessed 1.5.24. See also P. Trigo Kramcsák, Personal Data Protection and Data Transfer Regulation in Brazil, Chapter 1 of the compendium.

[126] See also Y. Zhang, n(2).

[127] See S. Parsheera, n(2).

SCC Modules

While models clauses developed by regions such as ASAEN or the Ibero-American network, may share similarities with EU SCCs, they are not exact replicas. [128] Most sets have two modules, with the GDPR SCCs including four modules and the China Standard Contract only one module.

Organising standard contractual clauses into modules driven by substantive requirements instead of roles with a view to more clearly identify the building blocks that would be necessary to achieve the highest common denominator and detect inconsistencies, would facilitate comparisons across sets of model clauses.[129]

Drawing inspiration from a variety of jurisdictions, e.g., the UK, Switzerland, and Brazil with its draft regulation on international data transfers, which highlights the importance of model clauses in supporting safe data exports and their flexibility, it is worth considering granting data protection authorities the power to evaluate the adequacy of model clauses adopted by other countries or international bodies and approve them, which could be done selectively module by module.

Comparing sets of model clauses, it is possible to extract at least eleven core substantive modules.

Model Clause Module	**Description**
Exporter's Obligations	The exporter should make sure the data was collected in a lawful manner prior to sharing the data with the importer. The exporter also remains accountable vis-à-vis the regulator and data subjects for complying with the local data protection framework.
Data Protection Safeguards Applicable to the Data Import	Data protection safeguards are controls that must be put in place by the importer, eventually with the help of the exporter, to achieve a wide range of data protection goals including lawfulness, purpose limitation, data minimisation, confidentiality, integrity, availability, accuracy, storage limitation, accountability, auditability.
Third Party Beneficiary Rights	Third party beneficiary rights are rights granted to data subjects so that they can intervene into the processing activities supported by these data flows, e.g., right to information, right to access, right to deletion, right to correction, restriction, right object, right not to be subject to automated decision-making, and more generally rights to enforce all or a substantial part of the clauses.
Restrictions on Onward Transfers, including Downstream Control of Processors and Sub-Processors	Restrictions on onward transfers are restrictions set upon the downstream use of the data, once the data is in the hands of the importer. In particular, when the importer uses the services of processors/sub-processors, it may be under an obligation to impose upon these entities the obligation to implement data protection safeguards that are not less restrictive than the safeguards found in the contract concluded with the exporter.
Importer's Assistance towards Exporter	Importer's assistance towards exporter relates to obligations imposed upon the importer to assist the exporter in its own compliance effort, e.g., to respond to data subject requests or to perform data protection impact assessments.
Importer's Obligations vis-à-vis Government Requests to Access Data	Clauses often govern the way the importer should handle requests to access data issued by public authorities, in particular for national security and law enforcement purposes by requiring that

[128] See Lee Matheson, n(85).
[129] See all references mentioned in n(85).

	the importer implement risk mitigation measures to the extent allowed by applicable law.
Exporter's Right to Audit Importer	The exporter's right to audit is a right to conduct some investigations, e.g., on the importer's premises, to determine whether the importer complies with the obligations set forth in the model clauses.
Model Clause Transparency Terms	Model Clause transparency terms grants, eventually under certain conditions, data subjects the right to access the content of model clauses and their annexes.
Importer's Submission to Exporter/data subjects' Supervisory Authority	Importer's submission to exporter's supervisory authority stems from the agreement of the importer to subject itself to orders issued by the data exporter/data subjects' supervisory authority to which it is the addressee.
Liability Terms	Liability terms set the liability standard and govern the relationship between the exporter and the importer when model clauses are breached.
Annex Content	The content of the annex relates to the actual description of data flows triggered by the exporter/importer relationship. The description can be more or less detailed depending upon the number of entries to populate and the level of granularity that is deemed acceptable for each entry.

Beyond the organisation into substantive modules, they are key concrete steps jurisdictions could take to enhance transparency and effectiveness by focusing on the often-neglected annexes to model clauses. These annexes are intended to provide a detailed description of the actual data flows involved in the transfer, yet they are frequently poorly drafted, leading to ambiguity and confusion. While the explanatory notes to the EU SCCs mention the possibility of adding multiple annexes for clarity, this is not a hard requirement. Here are few steps regulators could take to increase the level of transparency through SCC annexes:

1. Identify a typical list of processing purposes by role, e.g. billing, provision of service, personalisation of service, customer support, product/service improvement, auditing, and force parties to model clauses to map data types/categories to processing purposes.
2. Mandate a breakdown of processing purposes by role (e.g., controller or processor). By way of example, it is usually admitted that service improvement is pursued as controller and not as processor, while service provisioning and customer support is pursued as processor.
3. Mandate a breakdown of retention periods by role and processing purposes.
4. Make it clear that simply filling in model clauses by referring to the main agreement is bad practice.
5. Make it clear that once processing activities are broken down by processing purposes as listed in #1, there should not be any trade secret implication.

Recommendation:

Consider promoting a modular approach to SCCs based upon substantive requirements in addition to roles, making obligations to fill in annexes enforceable by third-party beneficiaries, and allocating resources to make annexes key transparency documents.

3.3.Industry Trends

While industry practices vary, notable trends emerge, in particular with the shift to cloud-based platforms for developing analytics and data science environments, as well as the growth of AI ecosystems. These trends

underscore the growing relevance of certification and model clauses and support the claim that the dichotomy between regulation and innovation is a false one.[130]

Data and Model Architectures

Industry practice now comprises both traditional Extract Transform Load (ETL) pipelines[131] and more flexible interactive query-engine pipelines that exemplify the modern data stack.[132] This is in this context that the data mesh industry movement[133] is of particular interest. A data mesh is a ”domain-oriented decentralized architecture for managing (analytical) data at scale. It enables the decomposition of an organization's monolithic analytical data space into data domains aligned with business domains. Such decomposition moves the responsibility of managing and providing high-quality data and valuable insights from the conventional central data teams into domain teams that intimately know the data.“[134] This shift is propelled by at least two factors: data quality assurances and allocation of data ownership, encompassing the responsibilities of data stewardship.[135]

What the data mesh approach implies is that the storage layer of a data architecture can in principle remain local. This way the data stays closer to its domain owner, a domain expert who is in charge of stewarding the data. The data also stays closer to the local data governance team, which is valuable from a legal and compliance standpoint, in particular from a data protection standpoint. Notably, keeping the storage layer local is not necessarily preventing security teams from operating globally, as long as a concept of low-risk data processing is introduced or acknowledged.[136] This approach makes it clear that it is misleading to think about data in terms of input only. Data is also an output, i.e., a result to a query.[137]

Consequently, the argument that data transfer restrictions are necessarily impeding innovation needs to be carefully nuanced,[138] and is ultimately dependent upon the use case at hand and the assessment of the output

---

[130] A. Bradford, The False Choice Between Digital Regulation and Innovation, Northwestern University Law Review, Vol. 118, Issue 2, October 6, 2024.

[131] An ETL pipeline is built to move the data from the source to the target, often a centralised data warehouse.

[132] Instead of waiting to receive the data, a data user writes a query that pulls in data directly from multiple sources at once. The utilization of an interactive query engine is a useful minimisation strategy as it can prevent data warehouses from the unnecessary storage of unused data and is particularly interesting for exploratory analytics on unfamiliar data sets or problems.

[133] Z. Dehghani, How to move beyond a monolithic data lake to a distributed data mesh in MartinFowler.com published on Many 20th 2019, available at https://martinfowler.com/articles/data-monolith-to-mesh.html, accessed 28.11.23, M. Schultze and A. Wider, Data mesh in practice – How to set up a data-driven organisation, O'Reilly Media Inc., available at https://www.oreilly.com/library/view/data-mesh-in/9781098108502/, accessed 28.11.23.

[134] Goedegebuure, A., et al. (2023). Data Mesh: a Systematic Gray Literature Review, arXiv:2304.01062 [cs.SE], p. 6.

[135] See e.g., J. Bode, N. Kühl, D. Kreuzberger, S. Hirschl, & C. Holtmann, Data Mesh: Motivational Factors, Challenges, and Best Practices, 2023, ArXiv [Cs.AI]; A. Wider, S. Verma, & A. Akhtar, Decentralized Data Governance as Part of a Data Mesh Platform: Concepts and Approaches 2023 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 2023, pp. 746-754; I. Araújo Machado, C. Costa & M. Yasmina Santos, Data Mesh: Concepts and Principles of a Paradigm Shift in Data Architectures Procedia Computer Science 196 (2022) 263–271.

[136] See S. Stalla-Bourdillon, n(4).

[137] This observation is further complicated by the fact that a model output could leak confidential training data. See V. Michael, R. Binns and L. Edwards, Algorithms that remember: model inversion attacks and data protection law Phil. Trans. R. Soc. 2018.

[138] The argument put forward is usually that “Restrictions on cross-border data transfers could slow AI development by limiting access to training data and important commercial services.” F. Schweitzer et al, The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade, White & Case Blog, 14 September 2023, available at https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules#:~:text=Restrictions%20on%20cross%2Dborder%20data,commercial%20services%20and%20foreign%20talent., accessed 28.11.23. Compare with this post by Mesh-ai available at https://www.mesh-ai.com/blog-posts/data-mesh-101-federated-data-governance, accessed 28.11.23.

that is generated. Importantly, there is a variety of use cases to consider, and frontier AI, i.e., the pre-training of large language models, is only a limited subset of the whole.

This decentralised architectural setting has three implications. First, data transfers can be reduced in size to cover 'insight' sharing (i.e., output sharing) as opposed to 'raw' data sharing (i.e., input sharing). In other words, data sharing can be made fine-grained. Such an approach makes sense from a data minimisation perspective (which is a data security requirement, even before being a data protection requirement).[139] Second, such an approach aligns with CETs, particularly those that rely upon the distinction between raw data and insight or inference.[140] Third and more importantly for our purpose, a decentralised architectural setting means that data governance can be federated: data governance rules can thus be set both at the global and local level. Rules related to which type of insight is useful to the recipient can be defined at the local level with minimum standards set at the global level. Rules related to data quality and data protection can be defined at the local level, with minimum standards set at the global level. In other words, it thus becomes easier to monitor compliance with SCCs or demonstrate that practice aligns with internal or public-facing policies to third parties.

Edge computing, a distributed computing paradigm,[141] is also worth mentioning: it involves processing data closer to the source of its generation, typically at or near the "edge" of the network, rather than relying on a centralised cloud server only to process the data.[142] Edge computing is nonetheless different from federated data architectures in the sense that it is primarily focused on optimising data processing at the edge of the network, and not on supporting collaborative data processing across decentralised entities.

Edge computing's uptake in industry can be attributed to various factors, starting with the proliferation of connected edge computing devices. Beyond this, three key elements explain the expansion of edge computing: first it addresses issues related to network congestion; second, the practical limitations and costs associated with transmitting substantial amounts of data make edge computing advantageous, as data relays are less often needed; third, certain applications demand extremely low latency, making it impractical to retrieve data from a distant cloud server. Edge computing therefore addresses these challenges by storing data in close proximity to the device, ensuring near-instantaneous access.[143]

Both federated data architectures and edge computing rely upon distributed processing, and, as long as devices are not locked up by operating systems, facilitate localised control over data. This is not to say that edge computing and federated data architectures do not raise their own challenges, in particular data and model security challenges, as well as unlinkability, which make certification all the more important in such contexts.

These trends confirm both the feasibility and relevance of conditional data transfers, e.g., to maintain data flows within a particular purpose perimeter or ensure data subject intervenability, and thereby the feasibility and relevance of a fine-grained approach to data transfers. A fine-grained approach to data transfer involves breaking down data flows into smaller, more granular, components based on specific criteria such as processing purpose, data types being consumed, and impact upon data subjects including violations of

[139] The least privilege principle is the security version of the minimisation principle and is now appearing in cybersecurity regulations, e.g. see the draft CCPA cybersecurity regulations.
[140] See S. Stalla-Bourdillon, n(4).
[141] As opposed to the centralized cloud computing paradigm. Unsurprisingly, there is much more research literature on edge computing than on the data mesh approach.
[142] Interestingly, the EU Data Act acknowledges this paradigm, which explains why under Recital 20 "[r]eadily available data does not include data generated by the use of a connected product where the design of the connected product does not provide for such data being stored or transmitted outside the component in which they are generated or the connected product as a whole."
[143] See e.g., D. Liu et al, Edge Computing Application, Architecture, and Challenges in Ubiquitous Power Internet of Things, Front. Energy Res., 22 February 2022, Sec. Smart Grids; K. Cao, Y. Liu, G. Meng & Q. Sun, An Overview on Edge Computing Research, in IEEE Access, vol. 8, pp. 85714-85728, 2020; W. Shi, J. Cao, Q. Zhang, Y. Li & L. Xu, Edge Computing: Vision and Challenges, in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.

fundamental rights and tangible and intangible harm. Rather than treating data transfer as a one-size-fits-all process, fine-grained data transfer emphasises the importance of context and tailored decision-making when allowing or refusing data transfers.[144] Such an approach confirms the ongoing relevance of DPAs and SCCs as well as certification.

AI Ecosystems

One other important consideration stems from the fact that AI-as-a-service does not rely upon standalone systems; it operates within complex ecosystems.[145] AI is more than a technology stack. AI services usually rely on a network of components, services, and stakeholders, which are highly integrated. Various stakeholders therefore interact with each other: developers design and build AI models, cloud service providers offer infrastructure and platforms for hosting AI services during development and deployment, hardware manufacturers produce the hardware components (e.g., GPUs, TPUs) used to accelerate AI computations, compute platforms offer capabilities to perform the computation on large scale, third-party tool providers offer specialised tools and software libraries to support AI development and deployment, and applications integrates AI-as-a-Service, often with a view to optimise service performance and user experience. AI ecosystems are also closely related to workforce ecosystems.[146]

What these complex ecosystems entail is the need to facilitate the production of meaningful pieces of trustworthiness evidence from a variety of stakeholders responsible for triggering multiple data and model flows. In such ecosystems, certification and DPAs with SCC extensions therefore remain fully relevant. The more complex the set of interactions, the more trustworthiness and trustworthiness evidence makes sense. The generative AI use case is particularly interesting for this matter. After the public release of generative AI services, e.g., ChatGPT, Copilot, Gemini, data and model security is now increasingly becoming an important differentiator, and unsurprisingly assurances are given through contract and certification. [147]

4.Data Transfer Tool Roadmap

As three levels of trustworthiness assurance coexist at the global level and some cross-border data transfer tools require more resources than others to become operable, it is useful to distinguish between short-term,

[144] See S. Stalla-Bourdillon, n(4), who explains why a fine-grained approach to data transfer would have the benefits of making the EU approach to data transfers more nuanced without undermining its rooting into the protection of fundamental rights. Interpreting Schrems II in this light, the same practical result as the result reached by the Facebook sage would however be reached, as Facebook was transferring bulk demographic and behavioural identifying data, which is an invaluable source for creating user profiles. Going further, it is doubtful whether SCCs and/or certification could ever be used to justify cross-border surveillance capitalism practices.

[145] See F. van der Vlist, A. Helmond, & F. Ferrari, Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence, 2024, Big Data & Society, 11(1) who monitor the industrialisation of AI and examine the convergence of AI and Big Tech, which they call Big AI. See also Crawford K (2021) Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press; Narayan D (2022) Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime. *Environment and Planning A: Economy and Space* 54(5): 911–929.

[146] Both highly-skilled workers and low-paid workers are part of these ecosystems. See B. Perrigo, Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic, 18 January 2023, Time, available at https://time.com/6247678/openai-chatgpt-kenya-workers/, accessed 1.4.25; J. Bartholomew, Q&A: Uncovering the labor exploitation that powers AI, 29 August 2023, Columbia Journalism Review, available at https://www.cjr.org/tow_center/qa-uncovering-the-labor-exploitation-that-powers-ai.php, accessed 1.5.24.

[147] See for example Einstein Copilot for Tableau, which leverages a Trust layer built into the Salesforce platform. This trust layer comprises security technology, and agreements, in particular contracts with third-party large language model (LLM) providers to achieve what is called “a zero data retention policy.” H. Ming, How Can I Trust Einstein Copilot for Tableau?, 2 April 2024, Tableau Blog, available at https://www.tableau.com/blog/how-can-i-trust-einstein-copilot-tableau, accessed 1.5.24.

mid-term and long-term policy goals when drawing a data transfer tool roadmap. These goals merit serious consideration by policy makers, even when they engage into digital trade negotiations.

Three Assurance Levels

To facilitate bottom-up converges between different national data protection regimes, it is crucial to consider more than just the data transfer tools themselves and check whether the minimum normative baseline being exported by the jurisdiction of the data exporter through the transfer tool does not impose additional requirements.

For instance, in the aftermath of the Schrems II decision, the EU introduced additional requirements to the Article 46 appropriate safeguards. This decision has been interpreted as mandating the implementation of supplementary measures when transferring data to third countries lacking essential guarantees against abuses by public authorities, such as surveillance and law enforcement agencies.[148] In other words, the CJEU's decision introduces a requirement to augment existing data transfer tools with supplementary measures to address potential shortcomings in data protection frameworks of destination countries.

In light of these considerations, it becomes possible to delineate three levels of assurance that are pertinent in the context of data transfers. ***Assurance level*** refers to a measure of the degree of trustworthiness or reliability associated with a particular system or entity in fulfilling its intended objectives or requirements. Assurance levels are often categorised based on the range of trustworthiness properties stakeholders should expect from a particular system or entity. Higher assurance levels indicate a wider range of properties, while lower assurance levels signify a more limited range of properties and thereby increased uncertainty or risk.

Firstly, the ***lowest*** assurance level entails ensuring that the data importer implements within the perimeter it controls adequate data protection safeguards to protect the transferred data. Secondly, a ***medium*** assurance level involves granting data subjects third-party beneficiary rights, allowing them to enforce their individual rights both against data exporters and data importers as well key data protection obligations imposed upon both parties. Of note, intervenability is becoming increasingly important in an age of AI and automated decision-making.[149] Yet, certification alone is not sufficient to support a right-based approach to data protection. Finally, the ***highest*** level of assurance necessitates the presence of either essential guarantees within the recipient country's legal framework or, at a minimum, the implementation of effective mitigation measures, including technical and organisational measures, to counteract the absence of such guarantees.[150]

As mentioned above, certification mechanisms play a crucial role in enhancing the trustworthiness and reliability of data processing activities, particularly at the lowest level of assurance. These certifications provide assurances that the data importer has implemented adequate data protection safeguards within their control perimeter to protect transferred data. By adhering to recognised standards and undergoing certification processes, organisations can demonstrate their commitment to data protection principles.

However, it is important to recognise that certification alone may not suffice to achieve assurance level 2, which involves granting data subjects third-party beneficiary rights. While certification can contribute to evidence that data importers have processes in place to respond to data subject requests, additional measures, such as implementing SCCs, are necessary to ensure that data subjects have the ability to enforce their rights against data exporters and data importers. SCCs can also make it possible to transform data subjects into enforcers of key data protection safeguards, beyond individual rights. Although SCCs are not

[148] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, Adopted on 18 June 2021.
[149] See e.g., S. Barros Vale and G. Zanfir-Fortuna, Automated Decision-Making under the GDPR – A Comprehensive Case Law Analysis, FPF Report, 17 May 2022, available at https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/, accessed 1.5.24.
[150] See S. Stalla-Bourdillon, n(4) for an evaluation of confidentiality enhancing technologies in the context of CBDTs.

substitute for certification, they thus provide a framework for accountability and enforcement that goes beyond what certification offers.

Furthermore, to attain assurance level 3, which requires either the presence of essential guarantees within the recipient country's legal framework or the implementation of effective mitigation measures, supplementary measures are essential. These measures are particularly critical when transferring data to third countries lacking adequate legal protections against potential abuses by public authorities, as highlighted in the aftermath of the Schrems II decision. Supplementary measures aim to ensure that the highest standards of data protection are maintained even in the absence of comprehensive legal frameworks. As explained in a previous report, CETs leveraged as supplementary measures should not be considered as mere substitute for CBDT tools and in particular SCCs, as fundamental trade-offs still need to be addressed within CET settings and CETs only aim to achieve narrowly-defined confidentiality objectives.

As a result, while certification is essential in that it makes it possible to lay the foundation for trust through the production of trustworthiness evidence describing data importers' actual practices and their alignment with internal and public-facing policies, SCCs and supplementary measures are indispensable for achieving higher levels of assurance in CBDTs.

Short v Mid and Long-Term Goals

To develop a roadmap for data transfer tools, we need to consider both the resources needed to develop them, their relative flexibility considering ease of adoption by parties to data transfers, and the level of harmonisation they would require to become effective. Here follows a breakdown of which tools should be prioritised in the near term, middle term, and long term.

Near Term: SCCs and Supplementary Measures

SCCs offer a low-resource, flexible and adaptable framework for data transfers, as they can be relatively quickly integrated into contracts, and tailored to specific business relationships and data transfer scenarios of which the details can be described in the annexes and supplementary questionnaires (which are often part of contractual negotiations). SCCs provide an immediate solution to introduce a wide range of safeguards. Allocating resources to enhance understanding, implementation, and monitoring of SCCs in the near term is thus a must do.

Supplementary measures encompass a range of technical and organisational safeguards that can be customised to address specific risks associated with data transfers, including encryption, pseudonymisation/anonymisation techniques, and contractual arrangements. Supplementary measures are crucial for ensuring the highest standards of data protection, particularly when transferring data to third countries lacking essential guarantees against abuses by public authorities. However, implementing effective supplementary measures requires careful assessment of risks, technical capabilities, and legal considerations. Therefore, allocating resources to research, develop, and implement robust supplementary measures tailored to priority data transfer user cases is imperative to address assurance level 3, which is not the same thing as simply endorsing the use of CETs. [151]

Mid Term: Certification

Certification mechanisms offer a standardised approach to demonstrate compliance with data protection regulations. They require a higher level of resources and harmonisation (when operated from the country of destination). However, they cannot achieve assurance level 2 on their own.

With this said, certification mechanisms offer powerful means to establish relational trustworthiness when they include an assessment of alignment of practices with organisational policies and effectiveness of controls, as opposed to mere contractual commitments. Therefore, in the mid-term, allocating resources to

[151] See S. Stalla-Bourdillon, n(4).

review, revise, or further develop certification mechanisms that that are comprehensive enough to provide strong assurances will be essential.

Long Term: Top-Down Harmonisation

Convention 108+ provides a framework for top-down harmonisation of data protection laws and standards across jurisdictions, making data transfer tools between member states unnecessary, although both DPAs and certification remain relevant for establishing relational trustworthiness between entities engaged into data sharing activities.

In the long term, prioritising efforts towards top-down harmonisation through Convention 108+ is essential for establishing a unified and coherent approach to data protection at the international level in particular between like-minded countries. Allocating resources to support and participate in Convention 108+ discussions, negotiations, and implementation efforts will contribute to the development of comprehensive and globally recognised data protection standards.

Recommendation:

Consider distinguishing between short, mid and long-term goals: 1) consider starting the roadmap by substantially investing in both developing and evaluating SCCs and supplementary measures and pushing for the harmonization of enforceability of third-party beneficiary rights; 2) consider continuing with the development of certification schemes that include an assessment of effectiveness of data protection controls; 3) consider pushing further for top-down harmonisation.

Free Trade and Global Data Governance Implications

Data protection and international law are closely linked by ongoing trade negotiations. These include bilateral and regional deals, and WTO talks, addressing cross-border data flows for digital commerce.[152]

At the multilateral level, it is important to highlight the Joint Statement Initiative (JSI) on Electronic Commerce, launched at the WTO's 11th Ministerial Conference in December 2017. Although it operates outside the WTO's formal multilateral negotiations, this plurilateral approach is being advanced by a subset of WTO members. The initiative's goal is to forge a legally binding agreement among its participants, addressing traditional trade issues such as trade facilitation, as well as a spectrum of digital policy concerns. These include CBDT and data localisation.[153]

The JSI has achieved consensus on several policy matters related to enhancing e-commerce. These matters encompassed e-signatures, e-contracts, spam regulation, and paperless trading.[154] In 2023, negotiations on cross-border data flows faced difficulties. A partial deal was made on data flows and localisation, with various approaches and proposals under consideration. Some members, led by Australia, Japan and Singapore championed provisions that enable and promote the flow of data,[155] with limited exceptions for "legitimate public policy objectives".[156] Additional provisions were discussed, such as the EU's proposal for an exception

[152] P. Trigo Kramcsák n(125).
[153] The WTO Joint Initiative on e-commerce (www.dig.watch), available at https://dig.watch/processes/wto-ecommerce, accessed 11.4.2024.
[154] Y. Ismail, Policy Analysis - Joint Statement Initiative on E-commerce at Crossroads for a "Substantial" Conclusion by MC13 (www.iisd.org, 17 July 2023), available at https://www.iisd.org/articles/policy-analysis/joint-statement-initiative-electronic-commerce, accessed 11.4.24.
[155] See, for example, 'WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore' (www.meti.go.jp, 20 January 2023) available at https://www.meti.go.jp/press/2022/01/20230120002/20230120002-3.pdf, accessed 10.4.2024.
[156] Y. Ismail, n(154).

related to privacy and personal data protection and Nigeria's proposal for policy flexibility aimed at developing and least-developed countries.[157] China presented a proposal aligned with commitments made in the Regional Comprehensive Economic Partnership (RCEP), expressing support for certain controls over data flows and data localisation requirements.[158]

In October 2023, the U.S. Trade Representative retracted its support for the United States' digital trade negotiation goals during the JSI discussions. This move implies abandoning the pursuit of international rules that would ensure the unrestricted flow of data across borders.[159] It also confirms that the protection of fundamental rights is not the sole public interest consideration that is capable of impacting upon approaches to CBDTs.

As regards CBDT tools for managing CBDT restrictions, SCCs are not mentioned in international trade agreements, contrary to certification schemes.

Some next-generation free trade agreements and digital partnerships, such as the USMCA,[160] the Digital Economy Partnership Agreement,[161] and the Singapore-Australia Digital Economy Agreement,[162] include provisions that acknowledge trustmarks or certification schemes as valid mechanisms for facilitating cross-border information transfers while safeguarding personal data (even promoting or encouraging participation in these mechanisms).

Although it is important to draw a clear distinction between free trade commitments and the protection of fundamental rights so that the former do not weaken the latter,[163] it seems possible to encourage the development, adoption and mutual recognition of comparable model clauses together with robust certification mechanisms. This does not necessarily imply condemning all local data handling requirements,[164] which seems to be a concern when they stem from human rights considerations and which are now emerging in the EU,[165] nor undermining the highest assurance level as an encouragement to develop does not

[157] Ibid.

[158] United Nations Conference on Trade and Development, 'What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce?: The Case of the Joint Statement Initiative' (2021) United Nations, available at https://www.un-ilibrary.org/content/books/9789210056366, accessed 11.4.2024.

[159] Broadbent, M. (2023). USTR Upends U.S. Negotiating Position on Cross-Border Data Flows. Center for Strategic & International Studies (CSIS). Retrieved from CSIS.

[160] The United States-Mexico-Canada Agreement, which substituted the North America Free Trade Agreement (NAFTA), provides in its Article 19.8 paragraph 6 that "[t]he Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information."

[161] The DEPA provides in its Article 4.2 paragraph 8 that "[t]he Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information."

[162] The SADEA provides in its Article 17.8 that "[t]he Parties recognise that the CBPR System is a valid mechanism to facilitate cross-border information transfers while protecting personal information."

[163] The European Data Protection Supervisor, in its opinion, for example raises the question whether "[c]onsidering that Japan has already been granted an adequacy finding by the Commission, (…) why, despite this adequacy decision, further negotiations on cross-border data flows were considered to be necessary." EDPS, Opinion 3/2024, n(22), para. 13.

[164] A. Vasudevan argue for example that "In light of existing inequalities in digital industrialization caused by the winner-take-all nature of the business, and the tendency of digital monopolists to hoard data, interventionist policies, such as some kind of data localization, may be necessary." A. Vasudevan, Global Data Flows Require a New Forum for Governance, 1 March 2023, Centre for International Governance Innovation Blog, available at https://www.cigionline.org/articles/global-data-flows-require-a-new-forum-for-governance/, accessed 1.5.24. India adheres to this view. See also S. Parsheera, n(2).

[165] See the provisional agreement on the European Health Data Space Regulation 2022/0140(COD), Article 60aa. It is explained that "[a] data localisation requirement within the Union for storage and processing is kept for secondary use with exceptions for third countries covered by adequacy decision," which reflects the view that adequacy decisions are the most robust CBDT tools.

necessarily imply that the CBDT tool will solve the data transfer conundrum in all cases. From a European perspective, it thus seems possible to both support the approach embedded within the EU horizonal model clauses[166] and an encouragement to the development of comparable model clauses.

Recommendation:

Consider encouraging the development, adoption and mutual recognition of comparable model clauses in the context of international agreements addressing cross-border data flows issues.

However, and this is an important consideration, building a new forum to discuss data privacy, data protection and more generally all types of public interests related to data governance is needed.[167] There are various reasons why negotiating data protection within free trade fora is problematic,[168] one important reason being that the underlying assumption in such fora is that it is sound to conceive human rights protection as a barrier to trade. It is also problematic to systemically assimilate public interest policies having an impact upon the free flow of data as barriers to trade.

The "data free flows with trust" (DFFT) initiative brought to the forefront by the Group of Twenty (G20)[169] has initially emerged as a response to the inadequacies of free trade fora.[170] The DFFT concept has now been taken up by the Group of Seven (G7) and the OECD,[171] and while being discussed in other international fora,[172] has been seen as an opportunity for extending certification schemes such as the CBPR System.[173] Yet, calls for strengthening trust are still loud and clear,[174] while some commentators still hope that the ""Institutional Arrangement for Partnership" could provide a forum to promote collaboration between the trade policy community, the digital and technology policy community and civil society."[175] At the same time, there is a

[166] Horizontal provisions for v cross-border data flows and for personal data protection (in EU trade and investment agreements), available at https://www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf, accessed 1.5.24.

[167] See A. Vasudevan, n(154). See also Svetlana Yakovleva, Kristina Irion, Pitching trade against privacy: reconciling EU governance of personal data flows with external trade, International Data Privacy Law, Volume 10, Issue 3, August 2020, Pages 201–221; Brännström, L. (2023). Global Inequality and the EU International Law Position on Cross-Border Data Flows. Nordic Journal of International Law, 92(1), 119-137.

[168] M. Kaminski, Why trade is not the place for the EU to negotiate privacy, 2015, Internet Policy Review, available at https://policyreview.info/articles/news/why-trade-not-place-eu-negotiate-privacy/354, accessed 1.5.24.

[169] G20 Osaka Leaders' Declaration 2019, available at https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html, accessed 1.5.24.

[170] A. Vasudevan, n(154).

[171] With the G7 Roadmap for Cooperation on Data Free Flow with Trust at the G7 Digital and Technology Ministers' meeting in April 2021 followed by the G7 Hiroshima Leaders' Declaration 2023, which endorsed the establishment of the Institutional Arrangement for Partnership (IAP).

[172] See e.g., the 18th UN Internet Governance Forum, in October 2023, available at https://www.intgovforum.org/en/content/igf-2023-outputs, accessed 1.5.24.

[173] See e.g., S. A. Aaronson, F. Kimura, H. Lee-Makiyama, S. M. Stephenson, Actions to make "data free flow with trust" operational in practice, Policy Brief submitted to the G20 TF4 -Digital Transformation Track, available at https://www.global-solutions-initiative.org/policy_brief/actions-to-make-data-free-flow-with-trust-operational-in-practice/, accessed 1.5.24; N. Cory, How the G7 Can Use "Data Free Flow With Trust" to Build Global Data Governance, 27 July 2023, Information Technology and Innovation Foundation Blog, available at https://itif.org/publications/2023/07/27/how-g7-can-use-data-free-flow-with-trust-to-build-global-data-governance/, accessed 1.5.24.

[174] B. Kilic, As Global Trade Goes Digital, Trust Becomes Critical, 29 February 2024, available at https://www.cigionline.org/articles/as-global-trade-goes-digital-trust-becomes-critical/, accessed 1.5.24.

[175] M. Morita Jaeger, Can trade policy enable "Data Free Flow with Trust?", 11 December 2023, Centre for Inclusive Trade Policy Blog, available at https://citp.ac.uk/publications/can-trade-policy-enable-data-free-flow-with-trust, accessed 1.5.24.

wider acknowledgement that "trade policy must respect the space for (…) domestic policymakers, regulators, enforcement officials, and legislators to debate and determine appropriate frameworks governing the relationship between government, technology, business, and the public interest,"[176] which raises the question whether the US and the EU approach to cross-border data flows are now finally converging. Looking at recent trade deals negotiated by the EU and in particular with Japan, a strong advocate of the DFFT initiative, some doubts remain.[177]

What our analysis shows is that unsurprisingly the DFFT means different things to different people and there is still a strong tension between proponents of an approach in terms of interoperability of legal frameworks which implies a relatively low normative baseline and proponents of a more inclusive approach who see some merits in some forms of soft and hard data localisation measures. Given the strong push towards extending the CBPR System globally, it is unclear whether the latter camp will manage to have enough space to voice its concerns.

Recommendation:

Consider making the Institutional Arrangement for Partnership an inclusive and multi-stakeholder arrangement, which should not limit itself to the promotion of the Global CBPR Framework.

5.Conclusion

In this paper, we have reviewed two CBDT tools, i.e., certification and SCCs, with a view to assess and compare their contribution in terms of trustworthiness, and in particular relational trustworthiness, i.e., trustworthiness built between parties to a data transfer, which we distinguish from institutional trustworthiness, i.e., trustworthiness derived from an assessment of the legal framework applicable to the data importer.

We explain how and why certification and SCCs are better viewed as complementary mechanisms and suggest that they should be combined together. Once it is acknowledged that SCCs are simply a subcategory or an extension of DPAs, it becomes harder to argue against their relevance, which does not mean that SCC templates are without criticism. We include five recommendations to improve SCC templates.

1. Identify a typical list of processing purposes by role, e.g. billing, provision of service, personalisation of service, customer support, product/service improvement, auditing, and force parties to model clauses to map data types/categories to processing purposes.
2. Mandate a breakdown of processing purposes by role (e.g., controller or processor). By way of example, it is usually admitted that service improvement is pursued as controller and not as processor, while service provisioning and customer support is pursued as processor.
3. Mandate a breakdown of retention periods by role and processing purposes.
4. Make it clear that simply filling in model clauses by referring to the main agreement is bad practice.
5. Make it clear that once processing activities are broken down by processing purposes as listed in #1, there should not be any trade secret implication.

[176] US Trade Representative Ambassador Katherine Tai, Remarks at the National Press Club on Supply Chain Resilience, June 2023, available at https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2023/june/ambassador-katherine-tais-remarks-national-press-club-supply-chain-resilience, accessed 1.5.24.

[177] C. Caffarra, B. Kilic, Re-joining trade with antitrust, 7 May 2024, VoxEU, available at https://cepr.org/voxeu/columns/re-joining-trade-antitrust, accessed 10.5.24 ("Although established as a non-negotiable redline, the EU first retreated in its agreement with the UK (…) and more recently with Japan, raising questions about the resilience of EU policy space.")

In practice, both certification and DPAs are actually regularly used by parties to data flows, even when no CBDT restrictions are applicable. In addition, several industry trends show that data governance approaches are getting more sophisticated and can accommodate decentralisation requirements, while data and model ecosystems are getting more complex, involving an increasing number of stakeholders and thus calling for governance mechanisms. These trends thus confirm the needs to contractually govern data flows and develop means to effectively demonstrate good practice beyond contractual commitments.

On the basis of these findings, we suggest a roadmap for CBDT tools, and responding to what seems to be a dominant view in the space, we argue that the short-term goal should be to invest in the development of SCCs and the deployment of a modular approach to SCCs based upon substantive requirements to facilitate cross-jurisdiction/region comparison and endorsement and more generally ease the identification of the highest common denominator.

Finally, we draw some implications in terms of free trade negotiation and global data governance, suggesting that free trade agreements should not treat SCCs differently from certification and that ultimately building a global data governance forum where a wide range of public policies are confronted is a fundamental next step. We caution against the reduction of the DFFT initiative to the global extension of the CBPR System.

In total, we make five main recommendations for policy makers, which are summarised below:

1. Consider incentivising competent authorities to make evidence on third countries rules and practices publicly available and eventually refer to relevant institutional trustworthiness metrics including contractual enforceability, enforceability of third party-beneficiary rights, and human-rights standards such as essential guarantees.
2. Consider promoting a modular approach to SCCs based upon substantive requirements in addition to roles, making obligations to fill in annexes enforceable by third-party beneficiaries, and allocating resources to make annexes key transparency documents.
3. Consider distinguishing between short, mid and long-term goals: 1) consider starting the roadmap by substantially investing in both developing and evaluating SCCs and supplementary measures and pushing for the harmonization of enforceability of third-party beneficiary rights; 2) consider continuing with the development of certification schemes that include an assessment of effectiveness of data protection controls; 3) consider pushing further for top-down harmonisation..
4. Consider encouraging the development, adoption and mutual recognition of comparable model clauses in the context of international agreements addressing cross-border data flows issues.
5. Consider making the Institutional Arrangement for Partnership an inclusive and multi-stakeholder arrangement, which should not limit itself to the promotion of the Global CBPR Framework.