cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

OPERATIONALISING PRACTICAL SOLUTIONS: A COMPENDIUM OF RESEARCH PAPERS

September 2024

Sophie Stalla-Bourdillon

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The Global Governance of the Digital Ecosystems (GGDE) project, within the framework of which this report has been prepared, received the support and/or input of CERRE member organisations. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

Table of Contents

ABOUT CERRE **4**

ABOUT THE AUTHORS **6**

INTRODUCTION TO THE CBDT RESEARCH COMPENDIUM **8**

STRUCTURE OF THE RESEARCH COMPENDIUM 10

COUNTRY DEEP DIVE 1: BRAZIL **12**

FOREWORD 13
1. INTRODUCTION 14
2. BRAZIL'S DATA PROTECTION MODEL 15
   2.1. Personal Data Protection as a Fundamental Right 15
   2.2. Relevant General Rules 16
   2.3. Brazil's comprehensive Data Protection Law: the LGPD 17
   2.4. Influence of the GDPR Model on the LGPD 18
   2.5. Core of the LGPD 20
   2.6. Data Retention and Data Localisation 26
   2.7. Surveillance and Law Enforcement Rules 28
3. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES 30
   3.1. Scope 30
   3.2. Data Transfer Tools 30
   3.3. Recent Evolution 31
4. INTERNATIONAL COMMITMENTS 34
5. CONCLUSIONS 41

COUNTRY DEEP DIVE 2: INDIA **43**

EXECUTIVE SUMMARY 44
1. CONTEXT 45
2. LEGAL FRAMEWORK ON DATA PROTECTION 48
   2.1. Evolution of the data protection law 49
   2.2. Scope of the DPD Act 50
   2.3. Rights and obligations 52
   2.4. Enforcement framework 53
   2.5. Data access for surveillance and law enforcement 53
3. INDIA'S POSITION ON CROSS-BORDER DATA FLOWS 54
   3.1. Data transfers under the DPD Act 55
   3.2. International arrangements 59
4. CONCLUSION 62

COUNTRY DEEP DIVE 3: CHINA **65**

FOREWORD 66
1. CONTEXT 66
2. CHINA'S DATA PROTECTION AND CYBERSECURITY MODEL 67
   2.1. Constitutional protection 68

2.2. Relevant general rules 69
2.3. Three main pillars of data protection and cybersecurity in China 70
2.4. Core Personal Data Protection Rules 72
2.5. Data localisation rules 78
2.6. Rules applicable to public authorities 78
3. CHINA'S CROSS-BORDER DATA TRANSFER REGIME 80
3.1. Scope 80
3.2. Data transfer tools 80
3.3. Recent evolution: the Provisions on Regulating and Promoting Cross-Border Data Transfers 85
4. INTERNATIONAL COMMITMENTS 86
5. CONCLUSIONS 88

CROSS-BORDER DATA TRANSFER TOOLS V. PRIVACY ENHANCING TECHNOLOGIES: A FALSE DEBATE 90

EXECUTIVE SUMMARY 91
1. INTRODUCTION 92
2. DATA-TRANSFER RESTRICTION PATTERNS 94
2.1. Restriction Pattern #1: "Bind the Intended Recipient" 94
2.2. Restriction Pattern #2: "Bind the Intended Recipient and Shield against Third Parties" 95
3. PETS AS SUPPLEMENTARY MEASURES 98
3.1. A PET typology 98
3.2. Fine-grained Data Transfer Assessment 107
3.3. Data Transfers, Trustworthiness, and PETs 111
4. CONCLUSION 112

RELATIONAL TRUSTWORTHINESS FOR CROSS-BORDER DATA FLOWS: ON CERTIFICATION AND MODEL CLAUSES 115

EXECUTIVE SUMMARY 116
1. INTRODUCTION 117
2. DATA TRANSFER TOOLS THROUGH THE LENSES OF TRUSTWORTHINESS 120
2.1. Conceptual Framing 120
2.2. Cross-Tool Comparison 126
3. DATA-TRANSFER TOOLS IN PRACTICE 130
3.1. Certification in Practice 130
3.2. Standard Contractual Clauses in Practice 137
3.3. Industry Trends 147
4. DATA TRANSFER TOOL ROADMAP 151
4.1. Three Assurance Levels 151
4.2. Short v. Mid and Long-Term Goals 153
4.3. Free Trade and Data Governance Implications 154
5. CONCLUSION 158

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE)

promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

- CERRE's added value is based on:
- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the Authors

Sophie Stalla-Bourdillon is Professor of IT Law and Co-Director of the Brussels Privacy Hub at the Vrije Universiteit Brussel (VUB). She is also visiting professor at the University of Southampton School of Law, where she held the chair in IT law and Data Governance until 2022.

Sophie is the author and co-author of several legal articles, chapters and books on data protection and privacy. She is Editor-in-chief of the Computer Law and Security Review, a leading international journal of technology law, and has also served as a legal and data privacy expert for the European Commission, the Council of Europe, the Organisation for the Cooperation and Security in Europe, and for the Organisation for Economic Cooperation and Development.

With contributions from Pablo Trigo Kramcsák, Smriti Parsheera, and Yuenming Zhang.

Pablo Trigo Kramcsák joined LSTS, VUB, Brussels, in January 2021 as a PhD student, funded by the "Becas Chile scholarship in digital transformation and technological revolution", awarded by the Chilean National Research and Development Agency.

He has over 8 years of experience as a Chilean government official (Chilean Transparency Council, Ministry of Foreign Affairs, National Consumer Service), dealing with information technology, e-commerce and privacy, cross-border data flows, and cybersecurity issues.

Smriti Parsheera is a lawyer and public policy researcher. She is currently pursuing a PhD in policy studies from the Indian Institute of Technology, Delhi. She has been a researcher at the National Institute of Public Finance and Policy, and a fellow at the CyberBRICS project.

Yueming Zhang is a postdoctoral researcher affiliated to the research group Law & Technology at Ghent University. She obtained her PhD degree from Ghent University in 2023. Her research focuses on privacy, data protection, and cross-border data transfers.

Introduction to the CBDT research compendium

This collection of policy papers has been prepared within the framework of CERRE's flagship project on "Global Governance for the Digital Ecosystems" (GGDE). It is in line with the project's overarching goal: to contribute to preserving and promoting regulatory convergence at the global level and, where convergence is neither desirable nor legitimate, to organise co-existence. This is the introduction of a series of papers examining how to pursue these objectives given both the increasing number of cross-border data transfer restrictions and increasing complexity.

Global trends show that cross-border data transfer (CBDT) restrictions are on the rise. Within each jurisdiction or region adopting or extending such rules, there is often an attempt to reconcile three competing interests: privacy and data protection, digital trade, and data sovereignty, with data sovereignty emerging as a proteiform concept that can be used to achieve multiple regulatory goals, including strategic economic autonomy, cyber resilience or national security. 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. It is thus clearly not sufficient to look at the 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 underlying trade-offs.

This complex landscape is illustrated by recent developments in several regions. Over the last six months, the European Commission has adopted the EU-US Privacy Framework and validated 11 pre-GDPR adequacy decisions, while aiming to accelerate the building of European Union (EU) data spaces and expressing concerns as regards the cross-border data transfer of non-personal data. The provisional agreement on the European Health Data Space Regulation introduces, for the first time, data localisation rules for the reuse of personal health electronic data. After having built a rather restriction cross-border data transfer regime, China has made public, through new provisions on CBDT, its willingness to ease its CBDT regime. India, with its new data protection law, has opted for a blacklist approach to CBDT, although sector-specific restraints will remain in effect. Brazil, which now appears to be a strong candidate for EU adequacy, recently announced a draft regulation related to international data transfers, which addresses adequacy decisions, contractual clauses and binding corporate rules. The United-States, with in particular the adoption of the executive order on preventing access to American' Bulk Sensitive Personal Data, recently introduced new data transfer restrictions, driven by national security interests.

This collection of research papers starts by doing a deep dive into three key jurisdictions: Brazil, India and China. It shows that all three jurisdictions have been or are still oscillating between competing regulatory goals and that lawmakers have attempted to preserve domestic policy spaces through the adoption of a complex set of CBDT restrictions, which can take the form of requirements to leverage a range of CBDT tools and/or to localise certain categories of data generated locally. CBDT tools can be conceived as legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained, once the data is handled by the data importer operating in a third country, e.g., adequacy decisions, Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification.

In such a fragmented context, strengthening multilateralism and global governance requires acknowledging diversity by developing a layered approach to CBDT tools and mapping these tools to a variety of assurance levels. It also requires complementing top-down efforts to feed convergence among like-minded jurisdictions and regions with wider bottom-up convergence efforts, i.e., efforts to push for the organic alignment of data processing practices through adoption of common standards by stakeholders involved in these practices and operating in or across regions.

This collection conceptualises CBDT tools as evidence of trustworthiness, be it institutional or relational trustworthiness. Institutional trustworthiness implies that trustworthiness is established at the jurisdictional level, once an analysis of the legal framework of the third country in which the data importer operates has been performed. Relational trustworthiness implies that trustworthiness is established at the entity level, once an assessment of the data importer's commitments and/or practices has been performed.

Emphasising the complementarity of CBDT tools, the collection lays the foundations for a roadmap that distinguishes between short, medium and long-term goals, as well as three distinct assurance levels in an attempt to accommodate for diverse approaches to CBDT. Assurance levels are usually categorised on the basis of a 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. 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 where possible, e.g., outside surveillance capitalism scenarios.

Besides, the collection also suggests that to fully comprehend the importance of CBDT tools for nurturing bottom-up convergence efforts, it is important to understand what privacy-enhancing technologies (PETs), or better confidentiality-enhancing technologies (CETs), really achieve in a cross-border data transfer context. The collection thus clarifies why CETs should not be considered as mere alternatives to CBDT tools and unpacks the security risk-assessment that underlies CET settings, which is, by definition, of a narrow focus and therefore still implies trade-offs.

The collection starts from the premise that model contractual clauses offer a flexible option for feeding bottom-up convergence in the short term even when there is no official acknowledgement of their relevance at the domestic level, e.g., in India, and highlight their complementarity with certification. At the end of the day, model clauses are data protection agreements and jurisdictions with no explicit CBDT restrictions often mandates the conclusion of contracts between parties exchanging data. At the same time, the collection shows that although certification is key for establishing relational trustworthiness, contractual commitments are still needed to grant third-party beneficiary rights, in particular to data subjects.

The collection thus suggests that in the short-term, resources should be allocated to the development of modular standard contractual clauses based upon substantive requirements (in addition to roles), to ease the endorsement at the domestic level of model clauses originating from other regions/jurisdictions.

Finally, the collection concludes by recommending that while bottom-up convergence efforts should be encouraged within free-trade negotiation fora, they should also be nurtured outside of these fora to enhance inclusiveness and address the variety of policy spaces that are emerging at the domestic level. Yet, it is unclear whether initiatives like the Institutional Arrangement for Partnership under the umbrella of the Data Free Flow with Trust policy drive have been built to address such a variety of concerns.

Structure of the research compendium

This workstream under the Global Governance for the Digital Ecosystems" (GGDE) project undertook deep dives into three key countries – Brazil, India and China. These countries were selected based on both geopolitical and economic importance, and each country case study unravels key drivers of how these actors intend to preserve their domestic policy spaces and to leverage the multilateral space. These deep dives contain at times important policy recommendations for policymakers from those countries, as well as lessons for those from other regions like the EU. They are organised in three preliminary chapters.

The fourth paper is on the flawed debate between the use of privacy enhancing technologies (PETs) and CBDT tools. CBDT tools are conceptualised as legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained, once the data is handled by the data importer operating in a third country, such as adequacy decisions, Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification but also adequacy decisions. They are conceived as a means to produce evidence of trustworthiness, which could be of two types: institutional trustworthiness or relational trustworthiness. This paper argues that the introduction of PETs, or better of a relatively narrow category of confidentiality enhancing technologies (CETs), does not reduce nor eliminate the need for CBDT tools. Although CETs provide an interesting way to address limited security threats on the condition that a holistic approach to data protection goals is adopted, the paper finds that CBDT tools are still needed to generate evidence of relational trustworthiness.

The fifth paper builds on the concept of relational trustworthiness, and the importance of two data transfer tools, model clauses (SCCs) and certification, as practical solutions for feeding bottom-up convergence. The paper reviews these two CBDT tools, with a view to assess and compare their contribution in terms of relational trustworthiness, i.e., trustworthiness that builds between two parties to a data transfer, which is distinguished from institutional trustworthiness, i.e., trustworthiness derived from an assessment of the legal framework in which parties to a data transfer operate. The paper distinguishes between three assurance levels in the context of data transfers and offers a roadmap for the development of CBDT tools. It also draws some conclusions as regards global data governance.

The authors would like to thank members of the steering committee and external reviewers for their precious feedback and in particular Graham Greenleaf, Alex Joel, Irene Kamara, Eric Lachaud, Malavika Raghavan, Nicolo Zingales, Ding Xiaodong, Benjamin Wong, Olivier Blazy, Theresa Stadler. All errors remain their own.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

COUNTRY DEEP DIVE 1: BRAZIL

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

Foreword

This policy report has been prepared within the framework of CERRE's flagship project on "Global Governance for the Digital Ecosystems" (GGDE). It is in line with the project's overarching goal: contribute to preserving and promoting regulatory convergence at the global level and, where convergence is neither desirable nor legitimate, to organising co-existence. It is the first of a series examining how to achieve these objectives in the case of cross-border data flows, with a country deep dive into the mechanisms to achieve cross-border data flows in the context of Brazil.

Brazil is a major global actor, leading South-South cooperation and forging strategic partnerships with China and the European Union (EU). The country holds a prominent position in the digital sphere, standing as Latin America's largest e-commerce market and an important hub for data centres. In response to the need for comprehensive data protection regulations, Brazil enacted the General Data Protection Law (LGPD) in September 2020. The EU General Data Protection Regulation (GDPR) served as a model for the LGPD, and both laws have many common features.

The LGPD is the cornerstone of Brazil's data protection framework. It presents a wide-ranging material scope and establishes a comprehensive set of data processing principles, rights, and obligations. Following the GDPR's approach, the LGPD has a broad extraterritorial reach. The Brazilian Data Protection Authority, the ANPD, plays a crucial role in overseeing compliance with LGPD provisions.

Chapter V of the LGPD addresses international data transfers, outlining specific guarantees and safeguards aimed at protecting the rights of individuals whose data is transferred abroad. Firstly, the LGPD allows such transfers if the destination country upholds an adequate level of protection, as determined by the ANPD.

In addition to countries with an adequate level of protection, the LGPD permits cross-border data transfers under specific circumstances. These include situations where the data controller provides and demonstrates guarantees of compliance with the principles, rights of data subjects, and the data protection framework outlined in the LGPD. Such guarantees can be achieved through controller's specific contractual clauses for a given transfer; standard contractual clauses (SCCs), prepared and approved by the ANPD, which establish minimum guarantees and conditions for carrying out an international data transfer; binding corporate rules; or seals, certificates and codes of conduct. The LGPD does not specify a hierarchical order among the available options for cross-border data transfers.

The ANPD released a draft regulation on data transfers on August 15, 2023. This draft establishes special requirements and guarantees for data exports, defines the content of SCCs, outlines the analysis process for specific contractual clauses and binding corporate rules, and specifies the adequacy decision assessment process for the data protection equivalence of foreign countries or international organisations. This draft also outlines procedures for the ANPD's recognition of equivalence for SCCs from other countries or international organisations. Additionally, it proposes a template for SCCs.

Standard contractual clauses will play a crucial role in the Brazilian personal data transfer framework, harmonising data protection obligations between data exporters and importers and ensuring compliance

with LGPD principles even when transferring data to countries lacking an adequacy status. The ANPD's draft regulation on data transfers outlines a simplified procedure for ANPD's recognition of equivalence for standard contractual clauses from other countries or international organisations (a process that may be initiated ex officio or upon the request of the interested parties), emphasising approval prioritisation for widely applicable SCCs.

1. Introduction

Brazil is one of the largest economies in the world, with a significant impact on international trade, investment, and economic cooperation. Its rich natural resources, varied industries, and emerging markets make Brazil a key player in shaping global economic trends and building collaborations.

As a leading country in Latin America, Brazil has promoted economic and diplomatic integration in the hemisphere. Moreover, Brazil is a key driver of the Southern Common Market (MERCOSUR) trade bloc, which aims to achieve economic integration with Argentina, Paraguay, and Uruguay.[1]

Beyond the Latin American sphere, Brazil holds significant political and economic sway as an emerging global power. It collaborates closely with China, India, and Russia, often through alliances such as the BRICS informal group. It is also a member of the G20, an intergovernmental forum that brings together the world's 20 largest economies. Brazil's strategic position in the World Trade Organization (WTO) aims to strengthen alternative global structures.[2]

Brazil maintains robust economic ties with major players such as China, the United States (US), and the EU. China serves as its principal trade partner. In 2022, their bilateral trade reached approximately USD 150 billion, absorbing nearly 27% of Brazil's export volume.[3] Brazil aims to enhance and broaden its trade connections with China.[4] The EU is Brazil's second-biggest trading partner, accounting for 18.3% of its total trade, and the biggest foreign investor in Brazil.[5] Brazil's South-South diplomacy has also placed significant importance on the African continent, particularly emphasising relationships with Portuguese-speaking African countries, Nigeria, and South Africa.[6] In this sense, Brazil has expanded its partnerships with

[1] Diana Roy, 'Brazil's Global Ambitions' (www.cfr.org, 19 September 2022) <https://www.cfr.org/backgrounder/brazils-global-ambitions> accessed 8 December 2023.
[2] William McIlhenny, 'A Brazil: A Voice for All?' (www.gmfus.org) <https://www.gmfus.org/news/new-geopolitics-alliances-rethinking-transatlantic-engagement-global-swing-states/brazil> accessed 9 December 2023.
[3] Salim Hammad, 'Brazil: Current Trade Patterns with China Threaten the Promise of Re-Industrialization' (www.economic-research.bnpparibas.com, 4 May 2023) <https://economic-research.bnpparibas.com/html/en-US/Brazil-current-trade-patterns-China-threaten-promise-industrialization-4/5/2023,48437> accessed 9 December 2023.
[4] McIlhenny (n 2).
[5] European Commission, 'EU trade relations with Brazil. Facts, figures and latest developments' (www.policy.trade.ec.europa.eu) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/brazil_en> accessed 9 December 2023.
[6] Marcus Vinícius de Freitas, 'Brazil and Africa: Historic Relations and Future Opportunities' (www.gmfus.org, 8 February 2016) ≤https://www.gmfus.org/news/brazil-and-africa-historic-relations-and-future-opportunities> accessed 9 December 2023.

various regional or sub-regional African organisations through bilateral agreements, reflecting its pursuit of a more proactive role on the continent.[7] Brazil is a significant player in the digital sphere, establishing itself as the largest e-commerce market in Latin America.[8] It is also the seventh most populous country in the world,[9] with a large digital community of about 181.8 million internet users,[10] ranking fifth globally.[11]

The country stands out as the primary data centre market in Latin America, attracting approximately 50% of the region's total investment. Sao Paulo is a key hub for Brazil's data centre facilities and hyperscale infrastructure. Leading cloud service providers such as AWS, Microsoft, Oracle, IBM, Tencent, and Huawei have a strategic presence in Brazil, offering private and public cloud services, mainly for the financial and government sectors.[12]

Brazil has been developing its regulatory frameworks to adapt to the digital era. In recent years, the country has enacted data protection laws to protect the privacy and rights of its digital citizens. The Brazilian General Data Protection Law, which follows the EU GDPR model, shows the country's commitment 'to increase the protection of personal data and regulate the way businesses collect, use, and process personal data'.[13] This legal framework regulates the processing of personal data, bringing Brazil in line with high international data protection standards.

2. Brazil's Data Protection Model

2.1. Personal Data Protection as a Fundamental Right

The interplay between international human rights law and Brazil's legal framework is particularly evident

[7] Christina Stolte, 'Brazil in Africa: Just Another BRICS Country Seeking Resources?', Chatham House Briefing Paper ≤https://www.chathamhouse.org/sites/default/files/public/Research/Africa/1112bp_brazilafrica.pdf> accessed 10 December 2023.

[8] Statista, 'E-commerce in Brazil - Statistics & Facts' (www.statista.com, 29 November 2023) ≤https://www.statista.com/topics/4697/e-commerce-in-brazil/#topicOverview> accessed 9 December 2023.

[9] Data based on the July 2023-July 2024 estimates from the United Nations' Department of Economic and Social Affairs, Population Division, World Population Prospects 2022. Worldometer, 'Countries in the world by population (2024)' (www.worldometers.info, 16 July, 2023) ≤https://www.worldometers.info/world-population/population-by-country/> accessed 6 February 2024.

[10] Statista, 'Number of internet users in selected Latin American countries as of January 2023' (www.statista.com, 24 February 2023) ≤https://www.statista.com/statistics/186919/number-of-internet-users-in-latin-american-countries/> accessed 8 December 2023.

[11] Statista, 'Countries with the largest digital populations in the world as of January 2023' (www.statista.com, 30 August 2023) ≤https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/> accesed 8 December 2023.

[12] Mordor Intelligence, 'Brazil Data Center Market Size & Share Analysis - Growth Trends & Forecasts up to 2029' (www.mordorintelligence.com) <https://www.mordorintelligence.com/industry-reports/brazil-data-center-market> accessed 9 December 2023.

[13] OneTrust DataGuidance and Baptista Luz Advogados, 'Comparing Privacy Laws: GDPR v. LGPD' (www.dataguidance.com, 9 August 2022) <https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-lgpd-0> accessed 14 December 2023.

in the context of personal data protection.[14] The 1988 Constitution of the Federative Republic of Brazil (Federal Constitution) establishes privacy as a fundamental constitutional right. Article 5(X) of the Federal Constitution safeguards the inviolability of individuals' privacy, private life, honour, and image. It also ensures the right to compensation for material and moral damages caused by violating these rights.

Additionally, on 10 February 2022, the Federal Senate approved Constitutional Amendment No. 115/2022, which explicitly added personal data protection -including in digital formats- to the fundamental rights outlined in Article 5 of the Federal Constitution. The amendment emphasises that the Federal Government has exclusive authority to oversee personal data protection issues, ensuring that only federal laws regulate the protection and processing of personal data. This centralised approach seeks to prevent inconsistency caused by different laws at the state and city levels.[15]

Furthermore, the Constitution contains the habeas data provision (Article 5(LXXII)(a)), which guarantees the rights of individuals to have access to their personal information contained in registries or databases maintained by the Federal Government or other public entities and to demand the correction of any incorrect data. The habeas data writ (regulated by the Habeas Data Law No. 9,507/1997) is a constitutional remedy and 'not strictly a substantive right, although this aspect can be inferred through its characteristics'.[16] It is worth noting that the habeas data writ 'has influenced other Latin American countries who have implemented similar data protection instruments'.[17]

2.2. Relevant General Rules

Brazil's general data protection and privacy framework encompasses several legislative sources, including the Brazilian Civil Code, the Consumer Protection Code, and the Internet Bill of Rights,[18] having 'more than

[14] Gabriel Oliveira de Aguiar Borges, 'Navigating Human Rights in the Digital Age: An Exploration of Data Protection Laws in Brazil and in Europe' (2023) 14 Beijing Law Review 1772.

[15] Angelica Mari, 'Data protection becomes a fundamental right in Brazil' (www.zdnet.com, 22 February 2022) ≤https://www.zdnet.com/article/data-protection-becomes-a-fundamental-right-in-brazil/> accessed 10 December 2023.

[16] Borges (n 14).

[17] Privacy International and Coding Rights, 'State of Privacy Brazil' (www.privacyinternational.org, 26 January 2019) <http://privacyinternational.org/state-privacy/42/state-privacy-brazil> accessed 7 December 2023.

[18] Coding Rights, Privacy LatAm and Privacy International, 'The Right to Privacy in Brazil - Stakeholder Report Universal Periodic Review 27th Session - Brazil' (2016) <https://privacyinternational.org/sites/default/files/2018-02/UPR27_brazil.pdf> accessed 7 December 2023.
Noteworthy laws in Brazil concerning data protection and access to information include the Credit Information Law, Law No. 12,414/2011, which governs how databases of payment information are created and accessed,
and the Access to Information Law, Law No. 12,527/2011, which limits the access to personal data stored in government databases when it poses threats to privacy and other individual rights (Carlos Affonso Pereira de Souza, Mario Viola and Ronaldo Lemos, 'Understanding Brazil's Internet Bill of Rights - 1st Edition' (2015) Instituto de Tecnologia e Sociedade do Rio de Janeiro. Available at https://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf). Regarding credit data, it is also worth mentioning the Brazilian Central Bank operates the Credit Information System (SCR), a credit bureau that gathers monthly data on credit operations from credit providers. This database includes customer and credit operation details for any amount above BRL 200. The National Monetary Council Resolution No. 4,571/2017 permits financial

40 laws and norms at the federal level'.[19] Notably, 'Brazil does have a strong civil law tradition and a developing consumer protection culture', with the Civil Code giving 'the contour the right to privacy, private life, home, correspondence and reputation'.[20] The Brazilian Civil Code, Law No. 10,406/2002, affirms privacy as an inviolable right of individuals, as specified in Article 21, and provides for civil remedies in cases of violation.[21]

The Consumer Protection Code (Law No. 8,078/1990) also regulates consumer data processing. It gives consumers the right to access their data, as specified in Article 43.[22] This legislation applies to the collection and administration of databases containing consumers' personal information, including Internet users.[23] Additionally, the Internet Bill of Rights (Law No. 12,965/2014) establishes principles, rights and obligations that service providers, including infrastructure and platforms, must follow. It contains specific rules related to processing personal data in online contexts.[24]

2.3. Brazil's comprehensive Data Protection Law: the LGPD

The Brazilian General Data Protection Law No. 13,709/2018 (Lei Geral de Proteção de Dados or LGPD)[25] came into effect on August 16, 2020, retroactively from its enactment on September 18, 2020. The journey toward establishing a comprehensive data protection law began in 2010 when the national consumer secretary of the Ministry of Justice presented a draft bill on data protection for public consultation.[26] Brazil lacked a comprehensive framework for protecting personal data before the LGPD came into effect. Previously, Brazil's data protection strategy relied primarily on sector-specific regulations, as discussed in earlier sections. This fragmented approach may have constrained Brazil's ability to thrive in the digital economy due to the absence of a unified, robust data protection framework. The introduction of the LGPD

institutions to access the aggregated information of each client in the SCR's database, with the client's consent (see Central Bank of Brazil, 'Credit Information System (SCR)' (www.bcb.gov.br) <https://www.bcb.gov.br/en/financialstability/creditinformationsystem> accessed 8 February 2024).

[19] Sarah Rippy, 'An Overview of Brazil's LGPD' (www.iapp.org, 18 September 2020) <https://iapp.org/news/a/an-overview-of-brazils-lgpd/> accessed 12 December 2023.

[20] Luiz Costa, 'A Brief Analysis of Data Protection Law in Brazil' (2012) Report presented to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) <https://rm.coe.int/a-brief-analysis-of-data-protection-law-in-brazil-report/168073d25f> accessed 9 December 2023.

[21] Timo Hoffmann and Pietro Luigi Pietrobon De Moraes Vargas, 'LGPD Et Al. – Report on the Law of Data Disclosure in Brazil' (2022) SSRN Electronic Journal <https://www.ssrn.com/abstract=4082390> accessed 9 December 2023.

[22] Privacy International and Coding Rights (n 17).

[23] DLA Piper, 'Data Protection Laws of the World - Brazil' (www.dlapiperdataprotection.com, 28 January 2024) <https://www.dlapiperdataprotection.com/?t=law&c=BR> accessed 6 February 2024.

[24] We will refer in detail to these provisions in section 2.6(a).

[25] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. An unofficial English translation is available at https://cyberbrics.info/wp-content/uploads/2020/02/The-Brazilian-LGPD-English-Version.pdf, translated Luca Belli, Laila Lorenzon and Luã Fergus.

[26] Robert Muggah and Pedro Augusto Pereira Francisco, 'Brazil's Data Protection Paradox' (www.cfr.org, 5 December 2019) <https://www.cfr.org/blog/brazils-data-protection-paradox> accessed 9 December 2023.

marks a crucial step in addressing these shortcomings, bridging gaps in privacy and data protection laws, and creating a legal environment that enables Brazil to fully realise its potential in the data-driven economy.[27]

The LGPD applies horizontally, and its far-reaching provisions cover the activities of data controllers and processors, establishing novel requirements for the processing of information of data subjects. The LGPD addresses various critical aspects, encompassing robust principles, guidelines for extraterritorial application, strong security measures, management of cross-border data transfers, mandates for appointing data protection officers and conducting data protection impact assessments. In this way, LGPD provisions 'uniform and complement the existing data protection framework'.[28]

The data protection law is enforced by the National Data Protection Authority (Autoridade Nacional de Proteção de Dados or ANPD). The LGPD vests the ANPD with extensive responsibilities concerning the interpretation, application, and enforcement of its provisions. Consequently, the effectiveness and success of this law rely heavily on the central role played by the ANPD.[29]

2.4. Influence of the GDPR Model on the LGPD

Brazil and the EU share strong historical, social, and economic bonds. Brazil was the first Latin American nation to forge diplomatic ties with the European Economic Community. Politically, Brazil and the EU acknowledge their roles as participants in a multipolar and evolving global system.[30] Strengthening relationships between the EU and Latin America is strategically important for Europe, and deepening ties with Brazil could unlock significant opportunities.[31] There has been a trend of replicating or transplanting European regulatory frameworks into the Majority World for various reasons, including what is known as the "Brussels Effect".[32] Brazil has endeavoured to 'align itself with international standards and references

[27] See OneTrust, 'What is the LGPD?' (www.cookiepro.com, 28 July 2020) <https://www.cookiepro.com/knowledge/what-is-the-lgpd/> accessed 9 December 2023.
[28] Privacy International and Coding Rights (n 17).
[29] Centre for Information Policy Leadership (CIPL) and Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP), 'The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD)' (2020) < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/%5Ben%5D_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd__04.16.2020__3_.pdf > accessed 9 December 2023.
[30] André Luiz Reis da Silva and Vitória Volpato, 'The Brazil-European Union Strategic Partnership: Advances, Convergences, and Challenges' Working Paper– October 2019 (2019) Leuven Centre for Global Governance Studies <https://ghum.kuleuven.be/ggs/research/eucross/eucross-wp-andre-reis-and-vitoria.pdf> accessed 9 December 2023.
[31] Antoni Comín i Oliveres, 'EU Needs Brazil for a New Global Strategy' (www.euractiv.com, 15 May 2023) <https://www.euractiv.com/section/global-europe/opinion/eu-needs-brazil-for-a-new-global-strategy/> accessed 9 December 2023.
[32] Renan Gadoni Canaan, 'The Effects on Local Innovation Arising from Replicating the GDPR into the Brazilian General Data Protection Law' (2023) 12 Internet Policy Review <https://policyreview.info/articles/analysis/replicating-gdpr-into-brazilian-general-data-protection-law> accessed 9 December 2023.

through these approaches'.[33] In that connection, 'the LGPD is largely inspired by the European data protection model'.[34]

The GDPR significantly influenced the Brazilian data protection law by exporting European data protection standards.[35] This impact is notably apparent in the broad integration of GDPR principles into the LGPD,[36] so much so that it is often referred to as Brazil's GDPR.[37] The LGPD aims to safeguard individual rights while fostering economic, technological, and innovative advancements by implementing clear, transparent, and comprehensive regulations for appropriately processing personal data. These objectives closely mirror the goals outlined in the GDPR.[38]

The LGPD comprises 65 articles that grant individuals specific rights regarding their data, impose responsibilities on organisations for the lawful processing of personal information, mandate the reporting of data breaches to both the supervisory authority and affected individuals, regulate the international transfer of data, and enforce penalties similar to those outlined in the GDPR. In this sense, the Brazilian data protection law replicates critical points of the European regulation. For instance, the LGPD presents a broad international scope, with Article 3 LGPD adopting the marketplace location principle, 'whereby the offering of goods or services or processing of data aimed at individuals located on Brazilian territory is enough for applicability'.[39]

However, it also contains some particularities that have been adapted to the Brazilian case. While 'the legal frameworks about data protection share foundational aspects across Brazil and Europe, cultural, historical, and legal contexts give rise to nuanced divergences in their implementation'.[40] For example, the Brazilian law creates ten legal bases allowing the processing of personal data, including credit protection. The credit protection lawful ground is specifically adapted to Brazil's credit sector's needs. Considering that the LGPD includes additional legal grounds for data processing, it could be possible to consider Brazil's data protection law 'as more flexible and less restrictive than GDPR in relation to the processing of personal data'.[41]

---

[33] Borges (n 14).
[34] Luca Belli and Nicolo Zingales, 'Brazilian Data Protection under Covid-19: Legal Certainty is the Main Casualty' (www.blogdroiteuropeen.com, 3 July 2020) <https://blogdroiteuropeen.com/2020/07/03/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty-by-luca-belli-and-nicolo-zingales/> accessed 12 December 2023.
[35] Canaan (n 32).
[36] Borges (n 14).
[37] Renato Opice Blum and Camilla Rioja, 'Brazil's "GDPR" Sanctioned with Extraterritorial Effects' (2018) IEEE Internet Policy Newsletter, September 2018 <https://internetinitiative.ieee.org/newsletter/september-2018/brazil-s-gdpr-is-approved-by-the-brazilian-house-of-representatives> accessed 11 December 2023.
[38] Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) 44 Brook. J. Int'l L. 859.
[39] Hoffmann and Vargas (n 21).
[40] Borges (n 14).
[41] Renato Leite Monteiro, 'GDPR Matchup: Brazil's General Data Protection Law' (www.iapp.org, 4 October 2018) <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/> accessed 14 December 2023.

2.5. Core of the LGPD

a) Personal Data under the LGPD

The LGPD has established a unified data protection framework, imposing general obligations across all sectors while 'systematizing the rights of data subjects'.[42] Within the LGPD, the concept of personal data is broadly defined, encompassing any information about an identifiable individual (Article 5(I)). This definition is not solely confined to information directly identifying an individual but also data that could potentially identify the person when aggregated with other information. Moreover, given their susceptibility to discriminatory practices, the LGPD introduces specific provisions targeted at sensitive personal data. This category includes personal data concerning racial or ethnic origin, religious beliefs, political opinions, trade union or religious, philosophical, or political organisation membership, health or sex life, and genetic or biometric data when linked to a natural person.

According to Article 12 of the LGPD, anonymised data is not deemed personal data, except in cases where the anonymisation process can be reversed through appropriate means or with reasonable efforts. The assessment of what constitutes 'reasonable' must consider objective factors, including costs, time, available technology, and the sole use of internal means required to reverse anonymisation. The ANPD may provide standards and techniques to be used in processes of anonymisation and security checks. It should be noted that according to Article 12, paragraph 2, 'the data used for formation of the behavioural profile of a given natural person, if identified, may also be deemed personal data'. Unlike the GDPR, the LGPD has not sufficiently systematised the concept of pseudonymisation,[43] nor has it formulated explicit incentives for its adoption by data processing agents.[44]

On January 30, 2024, the ANPD published -for public consultation, a Preliminary Study on anonymisation and pseudonymisation for data protection.[45] The study will inform the future guidelines on these topics, which aim to guide the processing agents on the legal impacts and the various techniques to anonymise or pseudonymise personal data. The study emphasises that anonymisation and pseudonymisation are not one-time actions, but continuous processes based on a risk approach. Therefore, they need to be constantly reevaluated to ensure that the risk of reidentification of the data subjects is acceptable, considering the speed of technological advancement, the availability of auxiliary data and the sophistication of possible attacks. The study mentions that any anonymisation process must be

[42] Hunter Dorwart, Mariana Rielli and Rafael Zanatta, 'The Complex Landscape of Enforcing the LGPD in Brazil: Public Prosecutors, Courts and the National System of Consumer Defense' (www.fpf.org, 16 December 2020) <https://fpf.org/blog/the-complex-landscape-of-enforcing-the-lgpd-in-brazil-public-prosecutors-courts-and-the-national-system-of-consumer-defense/> accessed 12 December 2023.

[43] Pseudonymization is defined in Article 13, paragraph 3, LGPD as the processing by means of which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment.

[44] Bruno Bioni, 'Compreendendo o conceito de anonimização e dado anonimizado. Direito Digital e proteção de dados pessoais' (2020) Cadernos Jurídicos. Ano 21 - Número 53 - Janeiro-Março/2020.

[45] Available at https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados

accompanied by documented risk management based on techniques to measure data reidentification risk, such as k-anonymity. These techniques must consider the cost and time required to reidentify the data, the context of the existing technologies, and the nature, scope, context and purpose of each processing operation. Finally, the study provides examples of anonymisation and pseudonymisation techniques in Annexe II, based on the type of data, distinguishing between structured text and images.

In addition, it's worth noting ANPD Technical Note No. 46/2022/CGF/ANPD from May 2022.[46] In this note, the ANPD makes some considerations regarding the anonymisation process and recalls that anonymisation is neither a panacea nor the only form of data protection.[47] It notes that anonymisation does not reduce the probability of re-identification of a data set to zero. Although complete anonymisation is a desirable objective from a personal data protection perspective, in some cases, this is not possible and must be considered a residual risk of re-identification (point 5.21). Moreover, the ANPD explicitly mentions two anonymisation techniques: k-anonymity (point 5.24) and differential privacy (point 5.25).

b) Scope

The LGPD applies broadly to any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarters is located or where the data are located. The term "processing" is extensively defined in Article 5(X) and covers a wide range of activities involving personal data. These activities include collecting, producing, receiving, classifying, using, accessing, reproducing, transmitting, distributing, storing, deleting, evaluating, controlling, modifying, communicating, transferring, disseminating, or extracting information.

Following the GDPR's approach, the LGPD exhibits a broad extraterritorial scope. As outlined in Article 3, the law applies to any processing activity, regardless of where the organisation collecting the data is established, if: (i) the processing is carried out in Brazil; (iii) the processing aims to provide goods or services or to process data of people in Brazil; or (iii) the data has been collected in Brazil. Consequently, the location of the company's headquarters becomes irrelevant as long as one of these criteria is met, allowing full enforcement of the LGPD. Unlike the GDPR, which requires foreign companies to designate a representative in the EU (Article 27) when they are subject to its rules, the LGPD does not impose such an obligation on processing agents not established in Brazil.[48]

In Article 4, the law excludes the application of data processing regulations in specific scenarios, namely:

---

[46] Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf/view

[47] Luís Osvaldo Grossmann, 'ANPD manda MEC fazer relatório e sustenta que dados públicos fazem parte da LGPD' (www.convergenciadigital.com.br, 18 May 2022) <https://www.convergenciadigital.com.br/Governo/ANPD-manda-MEC-fazer-relatorio-e-sustenta-que-dados-publicos-fazem-parte-da-LGPD-60327.html?UserActiveTemplate=mobile> accessed 20 December 2023.

[48] Oliver Yaros, Cristiane Manzueto and Rodrigo Leal, 'Brazilian and European Data Protection Law Extraterritoriality Scope' (www.mayerbrown.com) <https://www.mayerbrown.com/en/insights/publications/2020/12/brazilian-and-european-data-protection-law-extraterritoriality-scope> accessed 8 February 2024.

(i) data processing made by a natural person for exclusively private and non-economic purposes; (ii) data processing made exclusively for journalistic, artistic or academic purposes; (iii) data processing made exclusively for the purposes of public security, national defence, the safety of the Country, or crime investigation and punishment activities (subject to specific legislation);[49] and (iv) 'data originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents or subject to international transfer of data with other country than the country of origin, provided the country of origin provides a level of personal data protection consistent with LGPD provisions'.[50]

It is important to mention that the LGPD does not completely exclude data processing for academic purposes. Processing agents still need to follow the conditions laid out in Article 7 (covering lawful bases and other requirements for processing personal data) and Article 11 (on the processing of sensitive personal data).[51] In reference to the circumstance described in Article 4(IV), which involves a type of transient data transfer, there is 'no equivalent provision in the GDPR',[52] involving a type of transient data transfer.

c) Data Processing Principles

The Brazilian General Data Protection Law embodies 10 fundamental principles (Article 6) that underpin the processing of personal data. These principles serve as the cornerstone of Brazil's data protection framework, advocating for purpose limitation, adequacy or compatibility of the processing with the purposes communicated to the data subject, necessity or data minimisation, free access to the data

[49] We will refer in detail to this provision in section 2.7.

[50] Luca Belli, Laila Lorenzon and Luã Fergus, 'The Brazilian General Data Protection Law (LGPD) – Unofficial English Version'. Available at https://cyberbrics.info/wp-content/uploads/2020/02/The-Brazilian-LGPD-English-Version.pdf. Accessed 8 February 2024.

[51] The LGPD does not define these academic purposes. There are uncertainties surrounding the definition and scope of data processing made exclusively for academic purposes. The ANPD's Guidance - Processing of personal data for academic purposes and for carrying out studies and research (2023) points out that this concept is closely tied to the exercise of academic freedom by professors, students, and researchers within research bodies or educational institutions, in environments that foster the exchange and discussion of ideas, such as classrooms, scientific congresses, and seminars. Partial derogation for academic purposes should be interpreted restrictively, applying only to situations where the processing of personal data is directly related to the exercise of academic freedom, and it would not apply if personal data processing served other purposes, even indirectly related to academic activities, such as administrative or commercial functions within educational institutions. (Andressa Girotto Vargas, Augusto Henrique Alves Rabelo, Diego Vasconcelos Costa, Fernando de Mattos Maciel, Gustavo Gonçalinho, Lucas Borges de Carvalho and Sabrina Fernandes Maciel Favero, 'Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas' (2023) ANPD Autoridade Nacional de Proteção de Dados (June 2023) Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf). At the same time, it can be estimated that the extent of this exclusion is not clear. For instance, the ANPD's Guidance - Processing of personal data for academic purposes and for carrying out studies and research, asserts (on page 22) that the fact that the processing of personal data for academic purposes to be supported by one of the legal grounds contained in Article 7 LGPD does not mean that other LGPD provisions are not applicable, mentioning, by way of example, provisions relating to the data subjects' rights.

[52] OneTrust DataGuidance and Baptista Luz Advogados (n 13).

subjects, data quality, transparency, data security, prevention of damage, non-discrimination and accountability.

d) Data Subject's Rights

Brazil's data protection law grants individuals a set of 9 rights (Article 18), empowering them to exert control over their personal data vis-à-vis both public and private entities subject to the LGPD. These rights are the right to be informed about the existence of the processing; the right to access the data; the right to correct inaccurate, incomplete, or out-of-date data; the right to block, anonymise, or delete excessive or unnecessary data or data that is not being processed in compliance with LGPD; the right to the portability of data to another service by an express request; the right to deletion of personal data which is processed with the consent of the data subject; the right to information about private and public entities with which the data is shared; the right to be informed about the possibility of denying consent and the consequences of such denial; and the right to revoke their consent.

Data subjects are afforded additional rights elsewhere in the LGPD.[53] For example, Article 8 ensures accessible and transparent access to comprehensive information concerning the processing of personal data, mandating clear and adequate disclosure. Meanwhile, Article 20 gives data subjects the right to request a review of decisions made solely based on the automatised processing of personal data that affects their interests, including decisions designed to define their personal consuming habits and credit profile or aspects of their personality. It is framed as a 'right to review', 'thereby allowing for indirect control' of automated decision making.[54]

e) Lawful Grounds for Data Processing

The LGPD establishes 10 legal bases for lawful data processing (Article 7): (i) data subject's consent; (ii) for compliance with a statutory or regulatory obligation by the controller; (iii) by the public administration, for the processing and shared use of data required for the performance of public policies set forth in laws or regulations or supported by contracts, agreements or similar instruments; (iv) for conducting studies by research bodies,[55] guaranteeing, whenever possible, the anonymisation of personal data; (v) when

[53] Belli, Lorenzon and Fergus (n 50).

[54] Hoffmann and Vargas (n 21). 'The wording of this provision seems to suggest a wider protection than the relevant Article 22 of the GDPR which requires that the decision "has a legal effect or significantly affects the data subject"' (Katerina Demetzou, 'At the Intersection of AI and Data Protection Law: Automated Decision-Making Rules, a Global Perspective (CPDP LatAm Panel)' (www.fpf.org, 30 July 2021) <https://fpf.org/blog/at-the-intersection-of-ai-and-data-protection-law-automated-decision-making-rules-a-global-perspective-cpdp-latam-panel/> accessed 20 December 2023.). However, the provision of Article 20 of the LGPD would not operate as a general prohibition of individual decisions based 'solely' on automated processing.

[55] Although the LGPD establishes a more flexible legal regime for the processing of personal data for research purposes, it does not explicitly define the concepts of "study" or "research". It should be noted, however, that Article 5 offers a narrow definition for a 'research body.' This is relevant, given that the 'legal basis of 'research' is only valid for studies conducted by research bodies that meet the definition' (OneTrust DataGuidance and Baptista Luz Advogados (n 13)). According to Article 5(XVIII) LGPD, a research body is a 'body or entity of the direct or indirect public administration or not-for-profit legal entity governed by private law organized under the Brazilian laws, with its headquarters in Brazil, that includes basic or applied research of a historical, scientific, technological or statistical

necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject; (vi) for the regular exercise of rights in lawsuits, administrative or arbitration proceedings; (vii) for the protection of the life or of the physical safety of the data subject or of third parties; (viii) for health protection, exclusively, in a procedure performed by health professionals, health services or health authorities; (ix) when necessary to serve the legitimate interests of the controller or of third parties, except where the fundamental rights and liberties of the data subject prevail; and (x) for the protection of credit.[56]

These requirements come hand in hand with strict obligations for organisations to uphold mandatory and transparent disclosures within their privacy policies. Further, the law delineates special provisions for the processing of sensitive personal data (Article 11) and children's data protection (Article 14). Due to the sensitivity of this information, the LGPD outlines limited circumstances under which such data may be processed.[57]

f) Data Protection Authority

The National Data Protection Authority of Brazil operates as a federal public administration body. Provisory Measure No. 1124/2022,[58] later transformed into Law No. 14,460/2022,[59] brought changes to the LGPD and transformed the ANPD into a 'special nature autarchy'.[60] This change granted the ANPD

character in its institutional mission or bylaw'. When research bodies engage in data processing for purposes other than conducting studies, they must rely on a different legal basis (Andressa Girotto Vargas, Augusto Henrique Alves Rabelo, Diego Vasconcelos Costa, Fernando de Mattos Maciel, Gustavo Gonçalinho, Lucas Borges de Carvalho and Sabrina Fernandes Maciel Favero, 'Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas' (2023) ANPD Autoridade Nacional de Proteção de Dados (June 2023) Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf).
Regarding sensitive data, Article 11 LGPD establishes that this category of data can only be processed in certain circumstances without the supply of the data subjects' consent, including when this is essential for the conduction of studies by research bodies, 'guaranteeing, whenever possible, anonymization of the sensitive personal data (Article 11(II)(c)). In addition, article 13 LGPD states that in the 'conduction of studies on public health, the research bodies may have access to personal databases, which shall be exclusively processed within those bodies and for the sole purpose of conduction of studies and researches, and they must always be kept in a controlled and safe environment, according to the security practices set forth in the specific regulations and which include, whenever possible, the anonymization or pseudonymization of the data, and which consider the due ethical standards relating to studies and researches.'

[56] Belli, Lorenzon and Fergus (n 50).

[57] Rippy (n 19).

[58] Available at https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=2&data=14/06/2022

[59] 'Congresso Nacional promulga a Lei nº 14.460 que transforma a ANPD em autarquia de natureza especial' (www.gov.br, 26 October 2022) <https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial> accessed 14 December 2023.

[60] Fraga, Bekierman & Cristiano Advogados, 'Transformation of the ANPD into an Autarchy' (www.fblaw.com.br, 5 August 2022) <https://www.fblaw.com.br/en/transformation-of-the-anpd-into-an-autarchylgpd-express-01-22>accessed 14 December 2023.

autonomy and independence in making decisions and issuing normative publications. Subsequently, Presidential Decree No. 11,348/2023 connected the ANPD to the Brazilian Ministry of Justice and Public Safety. This action ended its previous direct affiliation with the Presidency of the Republic.[61] Constituted at the end of 2020, it is considered an independent data protection authority,[62] with a 'solid regulatory and personnel structure'.[63]

ANPD objectives encompass various aspects, including:

- Interpreting and clarifying the LGPD.
- Developing regulations for LGPD application and staying updated with evolving technologies and trends.
- Collaborating with other regulatory bodies and overseeing public authorities subject to the LGPD.
- Evaluating other jurisdictions to assess if they adequately protect data subjects' data.
- Regulating cross-border data transfers.
- Handling data subjects' complaints and enforcing the LGPD.
- Conducting investigations, holding hearings, and enforcing sanctions and penalties against organisations that violate the LGPD.

g) Other Elements

LGPD's Articles 37 to 40 define duties in processing personal data: record-keeping,[64] Data Protection Impact Assessments (DPIAs) at the request of the ANPD,[65] obligations to notify specific events such as data breaches, and proper processing practices. All controllers (public or private entities processing personal data) must appoint a Data Protection Officer (DPO), though there are certain exceptions for small businesses.

---

[61] Laura Drechsler, Isabela Maria Rosal Santos, Abdullah Elbi, Elora Fernandes, Eyup Kun, Bilgesu Sumer and Sofie Royer, 'Government access to data in third countries II - Brazil' (2023) European Data Protection Board. Available at https://edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf.

[62] See Opinion of the European Data Protection Supervisor of 3 May 2023 on the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and Brazilian law enforcement authorities (EDPS Opinion 14/2023). Available at: https://edps.europa.eu/system/files/2023-05/2023-05-03_edps_opinion_14-2023_brazil_en.pdf

[63] Drechsler et al. (n 61).

[64] While the GDPR precisely outlines in Article 30 the information to be recorded, the LGPD lacks specific details in this regard (OneTrust DataGuidance and Baptista Luz Advogados (n 13)).

[65] According to Article 5(XVII) LGPD, the DPIA is a document elaborated by the controller that contains a description of the personal data processing processes that could generate risks to civil liberties and to fundamental rights, as well as measures, safeguards and mechanisms to mitigate these risks. Even though they are not initially mandatory, DPIAs must be provided to the ANPD upon request (Article 38 LGPD).

When there is a breach of the LGPD by a controller or data processor, they face redress mechanisms and administrative sanctions imposed by the ANPD. The potential administrative sanctions include imposing fines of up to 2% of the entity's income in Brazil in the last fiscal year, capped at R$ 50,000,000 for the violation, suspending the processing of data associated with the violation until rectification, and mandating the deletion of personal data linked to the violation (Article 52 LGPD). According to Article 22, the defence of data subjects' interests and rights may be exercised in court, individually or collectively. Article 42 of the LGPD establishes civil liability for the controller or processor engaging in data processing activities that result in property, moral, individual, or collective harm due to violations of the law.[66]

2.6. Data Retention and Data Localisation

There is no provision for data localisation in Brazilian federal law. There are sectoral regulations that include 'data localization as a requirement for public procurement contracts involving cloud-computing services'.[67] These provisions are found in norms of the Secretary of Information Technology of the Ministry of Planning, Development, and Management 'regarding government contracts related to information and communications, which may include encryption methods, firewalls, and other measures. According to these rules, confidential data or information produced or safeguarded by the Federal Public Administration, including backup data, shall be physically located in Brazil'.[68]

a) Internet Bill of Rights

Brazil's Internet Bill of Rights, Law No. 12,965/2014,[69] provides for broad internet users' rights like the protection of their privacy and private communications, the protection of personal data, the right to obtain information on the collection, storage and processing of their data, the right to erase data, among others. The Internet Bill of Rights emphasises key privacy protection principles, notably affirming privacy rights (Article 3). It acknowledges the confidentiality of online communications, permitting exceptions solely through court orders in criminal investigations or procedures (Article 7(I)).

Moreover, it guarantees the right to accessible and transparent privacy policies (Article 7(IV)).[70] Article 11 establishes that '[a]ll operations involving the collection, storage, retention or processing of records, personal data, or communications by Internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records, if any of those acts occur in Brazilian territory'. The law includes a

[66] Henrique Fabretti Moraes and Rony Vainzof, 'Study Analyzes How Brazilian Courts Apply the LGPD' (www.iapp.org, 15 February 2023) <https://iapp.org/news/a/study-analyzes-how-brazilian-courts-apply-the-lgpd/> accessed 12 December 2023.

[67] Nigel Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?' (2017) Information Technology & Innovation Foundation. Available at: https://www2.itif.org/2017-cross-border-data-flows.pdf.

[68] Gabriel Aleixo Steibel Andréa Guimarães Gobbato, Isabela Garcia de Souza, Natalia Langenegger, Ronaldo Lemos and Fabro Steibel, 'The Encryption Debate in Brazil' (2019) Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

[69] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[70] Luiz Costa, 'A Brief Analysis of Data Protection Law in Brazil' (2012) Council of Europe. Available at https://pure.unamur.be/ws/portalfiles/portal/14199129/A_Brief_Analysis_of_Data_Protection_Law_in_Brazil.pdf

requirement that internet service providers and other internet services retain user data for a year and six months respectively.[71] In this sense, the Internet Bill of Rights is 'a standard for the improvement of current practices of data retention in Brazil'.[72]

In 2016, Regulatory Decree No. 8,771/2016 was enacted to clarify some provisions of the Internet Bill of Rights.[73] This decree primarily focuses on preserving net neutrality while also tackling certain aspects of privacy and confidentiality. Specifically, it mandates the minimal retention of personal data and private correspondence.[74] The Regulatory Decree also provides for the obligation to safeguard personal data by means of adequate information security measures, including the adoption of strict control of the employees who access personal data (access control). In addition, it establishes rules on purpose limitation and adequate use of personal data when processed via the Internet, noting that data must be eliminated when it achieves the purposes of its processing.

b) Cybersecurity and Cloud Rules

On December 29th, 2023, Brazil published its National Cybersecurity Policy (Decree No. 11,856/2023)[75] 'to guide cybersecurity activities in the country'.[76] This policy defines a set of principles, including national sovereignty and the prioritisation of national interests. It also emphasises the guarantee of fundamental rights, particularly freedom of expression, protection of personal data, privacy, and access to information.

The decree establishes the National Cybersecurity Committee, which comprises representatives from government, civil society, academic institutions, and business sector organisations. This committee will play a key role in proposing updates to the National Cybersecurity Policy and developing a National Cyber Security Strategy as well as a National Cyber Security Plan.

Furthermore, in the financial sector, banking and finance institutions must also rely on cybersecurity and cloud requirements typically provided by regulatory agencies such as the Central Bank of Brazil (CBB). CBB Resolution No. 4,893/2021[77] and Resolution No. 85/2021[78] regulate how financial and payment institutions adopt cybersecurity measures, and the requirements for contracting cloud computing services, including data processing and data storage services.[79] In this sense, financial institutions can only

[71] Access Now Policy Team, 'A Bill of Internet Rights for Brazil' (www.accessnow.org, 26 March 2014) <https://www.accessnow.org/a-bill-of-internet-rights-for-brazil/> accessed 7 December 2023.
[72] Carlos Affonso Pereira de Souza, Mario Viola and Ronaldo Lemos, 'Understanding Brazil's Internet Bill of Rights - 1st Edition' (2015) Instituto de Tecnologia e Sociedade do Rio de Janeiro. Available at https://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf
[73] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm.
[74] Erickson (n 38).
[75] Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm
[76] Mattos Filho, 'Decree establishing Brazil's National Cybersecurity Policy enacted' (www.mattosfilho.com.br, 5 January 2024) <https://www.mattosfilho.com.br/en/unico/brazils-cybersecurity-policy/> accessed 10 February 2024.
[77] Available at https://www.bcb.gov.br/content/about/legislation_norms_docs/CMN_Resolution_No_4,893_2021.pdf
[78] Available at https://www.bcb.gov.br/content/about/legislation_norms_docs/BCB_Resolution_No_85_2021.pdf
[79] Fabio Ferreira Kujawski, Thiago Luís Sombra, Paulo Marcos Rodrigues, 'Cybersecurity regulation in Brazil: an

contract with cloud service providers that are established in countries that have an agreement with the Central Bank of Brazil (CBB). In addition, the countries where financial data is processed must be notified to the CBB.[80]

2.7. Surveillance and Law Enforcement Rules

Article 4(III) of LGPD states that the law 'shall not apply to the processing of personal data: [...] made exclusively for the following purposes: a) public security; b) national defence; c) safety of the country; or d) crime investigation and punishment activities'. Then, Article 4, paragraph 1, establishes that this kind of data processing 'shall be governed by a specific law, which shall contain proportional measures as strictly required to serve the public interest, subject to the due process of law, the general principles of protection and the rights of the data subjects set forth in this Law'. Paragraph 2 of the same article adds that private entities are barred from processing data mentioned in Article 4(III), 'except in procedures carried out by a legal entity governed by public law'. This process must be specifically notified to the ANPD and must adhere to the limitations set in paragraph 4. Paragraph 4 states that in no event can all personal data of the database set forth in Article 4(III) 'be processed by a person governed by private law', unless its capital is entirely owned by public entities. The ANPD holds the responsibility to provide technical opinions or recommendations regarding these exceptions. Moreover, it has the authority to request the entities in charge to conduct data protection impact assessments.

In light of this, '[a] future data protection law for public security and criminal prosecution will have to provide for proportionate and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject'.[81]

Considering the rule contained in Article 4, paragraph 1, LGPD, it is possible to argue that 'the principles of data protection must already be observed for these activities. The recent recognition of the fundamental right to the protection of personal data by the Brazilian constitution also reinforces the need for minimal safeguards for any processing of personal data in the country'.[82] While public intelligence, investigative, and criminal prosecution activities are not covered by the LGPD, Chapter V allows these activities as a legal basis for data transfers.[83]

Brazil has not yet approved specific regulations on personal data processing in law enforcement. 'Even though there were legislative initiatives to establish a law for regulating the topic, these are still in a very

overview' (www.lexology.com, 15 October 2021) <https://www.lexology.com/commentary/tech-data-telecoms-media/brazil/mattos-filho-veiga-filho-marrey-jr-e-quiroga-advogados/cybersecurity-regulation-in-brazil-an-overview> accessed 13 December 2023.

[80] ibid.

[81] 'In Brazil, the competence to deal with public security is shared between different levels of the federation and encompasses different bodies, which makes a unique analysis of the use of personal data by these institutions a complex task' (Drechsler et al. (n 61)).

[82] Drechsler et al. (n 61).

[83] ibid.

initial stage'.[84] One of these initiatives is the Personal Data Protection Bill for the exclusive purposes of state security, national defence, public security, and investigation and repression of criminal offences (Bill No. 1,515/2022),[85] based on a preliminary draft prepared by a commission of jurists.[86]

A relevant decision by the Brazilian Supreme Federal Court in September 2022 has implications for the legality of data sharing among public authorities. The decision concerned the consolidated cases ADI 6,649 and ADPF 695,[87] which challenged the presidential Decree No. 10,046/2019. The Decree aimed to enable the exchange and integration of data, including non-sensitive and sensitive personal data, among various public entities within the Federal Public Administration. To do so, the Decree created different levels of data sharing. Specific organs would have access to certain databases, as determined by public agents, based only on their confidentiality. The Decree did not define any specific purposes for data sharing.[88] The Court ruled that the federal government must revise the rules on data sharing and interoperability, in accordance with the constitutional right to data protection and privacy. The Court also set out a number of criteria that must be followed by the public administration when sharing data, such as limiting the data to the minimum necessary for the informed purpose and complying with the requirements, guarantees and procedures established in the LGPD, as far as compatible with the public sector.[89]

---

[84] Isabela Rosal Santos, 'Data sharing between Europol and Brazil: challenging negotiation' (www.law.kuleuven.be, 28 November 2023) <https://www.law.kuleuven.be/citip/blog/data-sharing-between-europol-and-brazil-challenging-negotiation/> accessed 20 December 2023.

[85] Available at https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300

[86] The Bill No. 1,515/2022 addresses data sharing in various scenarios, such as: between competent authorities, between a competent authority and a non-competent public entity, and between competent authorities and private legal entities. The draft does not limit the sharing of personal data between competent authorities and private entities for state security and national defence purposes. For public security purposes, the draft allows competent authorities to access personal data and databases controlled by private legal persons (art. 12) by any of the following means: legal provision; voluntary cooperation; or contract, cooperation agreement or similar instruments. For criminal investigation and prosecution purposes, the draft authorizes a broad range of data sharing (art. 18). Unlike public security purposes, the draft requires a request from the police chief or the Public Prosecutor's Office instead of a legal provision. The draft also allows data sharing through voluntary cooperation; contract, cooperation agreement or similar instruments; or a state intelligence technical channel (Cynthia Picolo Gonzaga de Azevedo, Eliz Marina Bariviera de Lima, Felipe Rocha da Silva, Gustavo Ramos Rodrigues, Luiza Corrêa de Magalhães Dutra, Paulo Rená da Silva Santarém and Victor Barbieri Vieira Rodrigues, 'Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022' (2022) Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), 17. Available at https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf).
It worth noting that the draft bill has been criticized for changing the initial proposal from the jurists' commission. This has led to concerns about how it affects people's fundamental rights, disrupts the balance between criminal procedure and data protection principles, and creates legal uncertainty (See Azevedo et al., 2022).

[87] Available at https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683585

[88] José Renato Laranjeira de Pereira and Thiago Guimarães Moraes, 'Data-hungry government in Brazil: how narratives about state efficiency became fuel for personal data sharing' (www.eu.boell.org, 7 June 2022) <https://eu.boell.org/en/2022/06/07/data-hungry-government-brazil> accessed 7 February 2024.

[89] Luís Osvaldo Grossmann, 'STF limita troca de dados entre órgãos públicos para impedir abusos' (www.convergenciadigital.com.br, 15 September 2022) <https://www.convergenciadigital.com.br/Governo/Legislacao/STF-limita-troca-de-dados-entre-orgaos-publicos-para-impedir-abusos-61448.html?UserActiveTemplate=mobile> accessed 7 February 2024.

3. Transfer of Personal Data to Third Countries

3.1. Scope

The transfer of personal data to foreign countries or international entities, as defined in Article 5(XV) LGPD, is regulated by Chapter V of the same law (Articles 33 to 36). The LGPD establishes various guarantees and safeguards to protect the rights of data subjects whose data are processed within the LGPD's scope (Article 3). If the third country or organisation receiving this data does not comply with these safeguards, it may jeopardise the fundamental rights and freedoms of the data subjects.[90]

These provisions regulate the transfer of personal data by a processing agent (the controller or the processor, as defined in Article 5(IX)), who may be a natural person or a legal entity of public or private law) to a data importer (another processing agent, located in a foreign country or which is an international organisation, who receives personal data from the exporter).[91]

3.2. Data Transfer Tools

Under the LGPD, international data transfers are permitted provided that the recipient country maintains an adequate level of data protection, a determination made by the ANPD. As per Article 34, this evaluation considers: (i) applicable laws in the destination country or international organisation; (ii) nature of the transferred data; compliance with personal data protection principles and rights; (iii) security measures aligned with regulations; (iv) legal and institutional safeguards for data protection rights; and (v) any other relevant circumstances for the data transfer.

Furthermore, beyond countries with an adequate protection level, the LGPD allows cross-border data transfers under specific circumstances, when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in the LGPD, in the form of: (i) controller's specific contractual clauses for a given transfer,[92] (ii) SCCs (prepared and approved by the ANPD to establish minimum guarantees and valid conditions for carrying out an international data transfer), (iii) global corporate rules,[93] or (iv) regularly issued seals, certificates and

[90] Thaís Duarte Zappelini, 'Guia de Proteção de Dados Pessoais: transferência internacional' (2020) Fundação Getulio Vargas (FGV). Available at https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Accessed 21 December 2023.

[91] This arises from the provisions contained in the ANPD draft Resolution of the Regulation of International Transfers of Personal Data (released on August 15, 2023, for public consultation).

[92] These specific clauses should clearly describe the relationship between the purposes of processing and the international transfer of personal data, indicating the LGPD authorizing hypothesis that substantiates the operation, specifying its purpose, detailing the responsibilities of processing agents and the flow of data, as well as how safeguards for the rights and freedoms of data subjects will be guaranteed. See Zappelini (n 90).

[93] 'The LGPD contains the concept of global corporate rules, which are analogous to binding corporate rules' (Linklaters, 'Data Protected - Brazil' (www.linklaters.com, February 2024) <https://www.linklaters.com/en/insights/data-protected/data-protected---brazil> accessed 10 February 2024).

codes of conduct.

In addition, cross-border transfers are permitted when: (i) it is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities;[94] (ii) it is authorised by the ANPD; (iii) it is necessary for public policies or public service activities; (iv) data subjects have provided specific and highlighted consent for the transfer upon prior information;[95] (v) it is necessary for the fulfilment of a legal or regulatory obligation on the part of the controller; (vi) it is for a contract or procedures related to a contract in which the data subject is a party, as required by the data subject themself; or (vii) it is for the regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

According to Article 35, the ANPD is responsible for defining the content of SCCs and verifying the specific contractual clauses for any transfer, as well as the global corporate rules, seals, certificates and codes of conduct. These clauses and rules must comply with the LGPD's rights, guarantees, and principles. Additionally, the ANPD may delegate the evaluation of these clauses and rules to certification organisations, provided these entities adhere to the ANPD's regulations and are subject to its oversight. The ANPD has the authority to examine and, if needed, modify or cancel the actions of the certification organisations if they don't align with the law.

In terms of international data transfers, the LGPD and the GDPR share some structural similarities but also exhibit differences. For instance, unlike the GDPR, the LGPD does not prescribe a hierarchical order for the available international data transfer tools.[96] Moreover, the LGPD 'does not provide for the international transfer of data on the basis of a register which is intended to provide information to the public, nor based on the legitimate interest of the controller'.[97]

As Brazil has not yet recognised another country as having an adequate level of data protection and, at the same time, has not yet had this recognition from foreign authorities, each data flow must be evaluated on a case-by-case basis.[98]

3.3. Recent Evolution

On August 15, 2023, the ANPD initiated a public consultation on the regulation of international personal data transfers.[99] This consultation addressed the draft Resolution of the Regulation of International

[94] It should be noted that while public intelligence, investigative, and criminal prosecution activities aren't covered by the LGPD, Chapter V allows these activities as a legal basis for data transfers (Drechsler et al. (n 61)).
[95] Regarding the word "highlighted", the clause relating to international data transfer cannot be in the middle of other clauses in the case of a contract and must be separate. See Zappelini (n 90).
[96] Drechsler et al. (n 61).
[97] OneTrust DataGuidance and Baptista Luz Advogados (n 13).
[98] Zappelini (n 90).
[99] Baker McKenzie, 'Brazil: Data Protection Authority Launches Public Consultation on Regulation of International Transfers of Personal Data' (www. insightplus.bakermckenzie.com, 24 August 2023) <https://insightplus.bakermckenzie.com/bm/intellectual-property/brazil-brazilian-data-protection-authority-launches-public-consultation-on-regulation-of-international-transfers-of-personal-data> accessed 12 December

Transfers of Personal Data and the Standard Contractual Clauses (SSCs) template prepared by the ANPD. The draft[100] proposes guidelines for data transfers, emphasising alignment with the Regulatory Agenda for the 2023-2024 biennium (ANPD Ordinance No. 35/2022),[101] which includes actions or initiatives related to international transfers of personal data.

The draft covers important aspects of international data transfers, focusing first on the roles of the data exporter and data importer. The data exporter is a processing agent, located in the national territory or in a foreign country, who transfers personal data to the importer (Article 3.I). Conversely, the data importer is a processing agent located in a foreign country or an international organisation that receives the personal data transmitted by the exporter (Article 3.II).

The draft defines in Article 3 the concept of "transfer" (processing operation through which a processing agent transmits, shares or provides access to personal data to another processing agent). Then, it distinguishes between international data transfer (the transfer of personal data to a foreign country or to an international organisation of which the country is a member) and international collection of data (the collection of the data subjects' personal data carried out directly by the processing agent located abroad). According to the draft's provisions, an international data transfer occurs when personal data moves from an exporter to an importer, distinguishing it from simple international data collection (Article 7 states that international data collection does not constitute an international data transfer).

According to Article 2, international data transfer should be carried out: (I) maintaining compliance with principles and data subjects' rights regardless of data location; (II) adopting simple, interoperable procedures that support global standards, economic development, and secure cross-border data flow; (III) implementing responsibility measures to guarantee compliance and accountability; (IV) ensuring transparent information provision to data subjects about transfers; and (V) employing appropriate security measures in line with data criticality and operational risks. Article 9 outlines that international data transfers must be carried out for legitimate, specific, and explicit purposes informed to the data subject, with no possibility of subsequent processing incompatible with such purposes. The transfer must be supported by one of the LGPD's lawful bases for processing.[102]

In general terms, the draft Regulation sets the requirements and guarantees for transfers, defines the content of SCCs, outlines the analysis process for specific contractual clauses and global corporate standards (binding corporate rules),[103] and establishes an adequacy decision mechanism for foreign countries or international entities' data protection equivalence. It also delineates communication

2023.

[100] Available at https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais

[101] Available at https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885

[102] Julio Cesar de Oliveira Alves and Rafael Scatamacchia, 'LGPD's five year anniversary and regulation on the international data transfers' (www.jdsupra.com, 5 October 2023) <https://www.jdsupra.com/legalnews/lgpd-s-five-year-anniversary-and-1036029/> accessed 13 December 2023.

[103] Chapters VI and VII of the draft indicate ANPD's understanding that global corporate standards are the equivalent to binding corporate rules under the GDPR (see de Oliveira Alves and Scatamacchia (n 102)).

procedures with the ANPD. It should be noted that the draft Regulation does not refer to seals, certificates and codes of conduct.

Article 15 of the draft states that the validity of the international data transfer based on SCCs presupposes the full adoption of the SCCs model prepared by the ANPD (contained in Annex II of the same draft Regulation) without any changes, in a contract between the exporter and the importer. The SCCs can also be part of a specific agreement or a larger agreement to regulate international data transfers.

Moreover, the draft outlines a simplified procedure for ANPD's recognition of equivalence for SCCs from other countries or international organisations (a process that may be initiated ex officio or upon the request of the interested parties), emphasising approval prioritisation for widely applicable clauses.[104] The ANPD 'has yet to recognize the equivalence of standard contractual clauses from other countries or international organizations'.[105]

The controller is ultimately responsible for fulfilling any legal obligations and contractual commitments, answering to ANPD's requirements, ensuring data subjects' rights and responding to any potential harm, regardless of whether the exporter or importer oversees some measures. Also, when both the exporter and importer are processors, the controller must sign the SCCs and take full responsibility for these obligations.[106]

It is important to note that in ANPD's draft SCCs 'the provisions relating to the rights of the data subject do not provide any limitations, such as those under the EU SCCs'.[107] For example, data subjects may file lawsuits against the exporter or the importer, as they choose, before the competent courts in Brazil.

Article 20 of the draft Regulation allows the controller to request the ANPD's approval for specific contractual clauses for a given transfer when it involves a unique international data transfer that cannot use the SCCs. This may happen because of exceptional circumstances, factual or legal, that the controller should justify. The specific contractual clauses must ensure and demonstrate compliance with the LGPD principles, the data subjects' rights, and the data protection framework set by the law and the draft.

Regarding global or binding corporate rules, the draft Regulation clarifies that they are intended for international data transfers between organisations of the same economic group, having a binding character upon all group members. It states that these corporate standards must be linked to establishing and implementing a privacy governance program, enumerating in Article 26 their requisites. These

[104] It is suggested that this recognition could include SCCs from the EU and the UK. See The Software Alliance (BSA) and the Global Data Alliance (GDA), 'Response to ANPD Consultation on International Data Transfers' (globaldataalliance.org, 25 September 2023) <https://globaldataalliance.org/wp-content/uploads/2023/09/09262023intldatatrans.pdf> accessed 13 December 2023.
[105] Baker McKenzie (n 99).
[106] Renata Neeser, 'Brazil Data Protection Agency (ANPD) Publishes Proposed International Transfer of Personal Data Regulation for Public Consultation' (www.littler.com, 16 August 2023) <https://www.littler.com/publication-press/publication/brazil-data-protection-agency-anpd-publishes-proposed-international> accessed 15 December 2023.
[107] ibid.

requirements encompass delineating the categories of personal data transferred, specifying the processing objectives, detailing legal frameworks, and identifying the recipient countries. Moreover, the standards must define the corporate structure and responsibilities within the group. They should also explicitly outline the rights of individuals whose data is being transferred and the procedures for exercising these rights, mandating the communication of any alterations to the pertinent data protection authorities.

Finally, on the adequacy decision mechanism, Article 12 specifies that the assessment of the level of protection of personal data 'shall address the risks and benefits provided by the adequacy decision, acknowledging, inter alia, the guarantee of the principles, the rights of data subjects, and the regime of data protection provided for in the LGPD in addition to the impacts on the international flow of data, diplomatic relations and international cooperation between Brazil and other countries and international organizations'. It also indicates that the 'ANPD shall prioritize the assessment of the level of data protection of foreign countries or international organizations that ensure reciprocal treatment to Brazil [...]'.

The ANPD conducted a public consultation on the draft Regulation for international data transfers until October 14, 2023. The authority plans to finalise the process in 2024.[108]

4. International Commitments

Brazil has ratified several international agreements involving privacy considerations. These include:

[108] Mattos Filho, 'International Data Privacy Day: an overview of the ANPD's efforts in 2023' (www.mattosfilho.com.br, 29 January 2024) <https://www.mattosfilho.com.br/wp-content/uploads/2024/01/one-pager-dia-internacional-protecao-de-dados.pdf> accessed 11 February 2024.

- The International Covenant on Civil and Political Rights (ICCPR): Article 17 protects against arbitrary or unlawful intrusion into privacy, family, home, correspondence, and unwarranted attacks on reputation and honour. The Human Rights Committee (the body of independent experts that monitors the implementation of the ICCPR) highlights the obligation of State Parties to the ICCPR to implement legislative measures to uphold these rights.[109]
- The American Convention on Human Rights, also known as the "Pact of San José de Costa Rica": Article 11 establishes that '[n]o one may be the object of arbitrary or abusive interference with his private life'.
- The Council of Europe Convention on Cybercrime (ETS No. 185): On 30 November 2022, Brazil acceded to the Convention on Cybercrime (Budapest Convention).[110] On 12 April 2023, the Brazilian President signed the corresponding legislative decree, by which Brazil finally adopted the Council of Europe Convention on Cybercrime.[111]

Furthermore, Brazil has actively contributed to advancing discussions at the United Nations regarding the right to privacy.[112] As regards the 'only binding international convention within the international privacy and data protection policy space',[113] Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), in 2018, Brazil joined the Committee of Convention 108 as an observer.[114] With the observer status, Brazil participates in the discussions and workings of the Committee of Convention 108, contributing to the global dialogue and cooperation on data protection and privacy rights.[115] The main goal of Convention 108 is to enable the free flow of information among Convention Parties and from Parties to non-Parties while safeguarding data protection beyond the jurisdictions of the Parties.[116] The Committee of Convention 108, during its 44th plenary

[109] Coding Rights, Privacy LatAm and Privacy International (n 18).
[110] 'Brazil Accedes to the Convention on Cybercrime and Six States Sign the New Protocol on E-Evidence' (www.coe.int, 30 November 2022) <https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence> accessed 11 December 2023.
[111] OFFICIALBLOGUNIO, 'Brazil's Recent Ratification of the Budapest Convention on Cybercrime' (www.officialblogofunio.com, 26 May 2023) <https://officialblogofunio.com/2023/05/26/brazils-recent-ratification-of-the-budapest-convention-on-cybercrime/> accessed 11 December 2023.
[112] Coding Rights, Privacy LatAm and Privacy International (n 18).
[113] Colin J Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession' (2020) CIGI Paper No. 246. Available at https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/
[114] 'Brazil and the Data Protection Commission of Gabon to Join the Committee of Convention 108 as Observers !' (www.coe.int, 12 October 2018) <https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers-> accessed 9 December 2023.
[115] On May 24th, during the 2023 Computers, Privacy and Data Protection International Conference (CPDP), a dedicated panel discussed the anticipated impact of the ratification of the Protocol CETS No 223 amending Convention 108 (also known as the modernised Convention 108 or Convention 108+). Organised by the Council of Europe, the panel included Juliana Muller, Head of International and Institutional Relations at the Brazilian National Data Protection Authority. Muller highlighted the ongoing discussions in Brazil regarding its potential accession to Convention 108. She emphasised that Brazil would now meet the necessary access criteria, specifically highlighting the provisions outlined in article 15.5 of the modernised Convention 108.
[116] 'Newsroom - Model Contractual Clauses for the Transfer of Personal Data (Module 1)' (www.coe.int, 27 June

meeting held in Strasbourg from 14 to 16 June 2023, adopted the first module of the Model Contractual Clauses for transborder data flows of personal data,[117] developed based on Convention 108+, for data flows from data controller to data controller.[118] At its 45th plenary meeting, the Committee of Convention 108 adopted the second module of the Model Contractual Clauses for transborder data flows of personal data,[119] which addresses the transfer of personal data from controller to processor.[120]

As LGPD incorporates numerous aspects akin to the EU GDPR, this alignment has prefigured Brazil's endeavours towards obtaining a mutual adequacy finding from the European Commission. In this regard, Brazilian and European Union authorities have been 'intensively working' on a mutual-adequacy arrangement for data flows,[121] based on the proximity of the European regulation and the Brazilian law, as explained by the ANPD president Waldemar Gonçalves.[122]

The European Commission is conducting several adequacy assessments for countries with similar data protection principles. Brazil is included among these potential partners, and EU Justice Commissioner Didier Reynders 'plans to travel to the country soon for expected negotiations'.[123] On 22 February 2023, the European Commission issued a Recommendation for a Council decision authorising the opening of negotiations for an agreement between the EU and Brazil on exchanging personal data between Europol and the Brazilian authorities competent for fighting serious crime and terrorism.[124] Regarding a possible GDPR adequacy finding, it is asserted that although the LGPD establishes a robust and extensive data protection framework, there is a need for comprehensive regulations about national security, public security, national defence, and criminal procedure.[125]

2023) <https://www.coe.int/en/web/data-protection/-/model-contractual-clauses-for-the-transfer-of-personal-data> accessed 13 December 2023.

[117] Available at https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4

[118] 'Newsroom - Model Contractual Clauses for the Transfer of Personal Data (Module 1)' (n 116).

[119] Available at https://rm.coe.int/t-pd-2023-4rev2-mcc-module-2-en-final/1680ad6a36

[120] 'Newsroom - Model Contractual Clauses for the Transfer of Personal Data (Module 2)' (www.coe.int) <https://www.coe.int/en/web/data-protection/-/model-contractual-clauses-for-the-transfer-of-personal-data-module-2> accessed 13 December 2023.

[121] Ana Paula Candil, 'Brazil, EU 'intensively working' on mutual-adequacy data flow accord, EU data chief says' (www.mlexmarketinsight.com, 6 November 2023) <https://mlexmarketinsight.com/news/insight/brazil-eu-intensively-working-on-mutual-adequacy-data-flow-accord-eu-data-chief-says> accessed 11 December 2023.

[122] Luís Osvaldo Grossmann, 'ANPD negocia adequação entre Brasil e União Europeia para transferência de dados' (www.convergenciadigital.com.br, 5 October 2023) <https://www.convergenciadigital.com.br/Governo/Legislacao/ANPD-negocia-adequacao-entre-Brasil-e-Uniao-Europeia-para-transferencia-de-dados-64414.html?UserActiveTemplate=mobile> accessed 11 December 2023.

[123] Jennifer Bryant, 'Reynders announces European Commission's latest international data transfer plans' (www.iapp.org, 16 November 2023) <https://iapp.org/news/a/reynders-international-cooperation-toward-safer-digital-future-a-necessity> accessed 14 December 2023.

[124] EDPS Opinion 14/2023 (n 62). In this regard, it is mentioned that unlike Article 6 of Convention 108+, the LGPD does not explicitly classify personal data related to criminal convictions as a special category. Consequently, Brazil lacks a more stringent protective framework for this data, potentially conflicting with the protection standards required by Convention 108+ Parties, such as the European Union (Rosal Santos (n 84)).

[125] Drechsler et al. (n 61).

On October 21, 2021, the ANPD announced its incorporation as a voting member within the Ibero-American Data Protection Network (RIPD).[126] The RIPD aims to promote the protection of personal data in Latin America by facilitating the sharing of information, experiences, and knowledge among its members. Furthermore, it endeavours to propel regulatory advancements to ensure a progressive and robust framework for safeguarding the right to personal data protection within democratic contexts. The RIPD published, on 20 June 2017, the Standards for Personal Data Protection for Ibero-American States.[127] These standards create a unified framework of data protection principles and rights applicable across the various national legislations within the Ibero-American region. On September 27, 2022, the RIPD released the Guide for Implementing Standard Contractual Clauses for International Personal Data Transfers.[128] This document outlines specific considerations for conducting international transfers of personal data using SCCs. It provides guidance for entities conducting data transfers from RIPD member countries to jurisdictions lacking adequate data protection measures.[129] This model 'does not create a binding legal obligation for the Network's member states to recognise its validity; instead, it offers a view of how national data protection regulators and policymakers in Latin America are collectively approaching the issue of cross-border data transfer tools'.[130]

Ongoing trade negotiations closely link data protection and international law. These include bilateral and regional deals, as well as WTO talks, all focused on the digital economy and cross-border data flows for digital commerce. The EU is a fundamental stakeholder in shaping global privacy regulations and safeguarding personal data.[131] 'From the perspective of the EU, unreservedly committing to free cross-

[126] 'EU and US Take Measures to See to the Implementation of the Data Privacy Framework' (www.privacylaws.com, 15 November 2023) <https://www.privacylaws.com/news/eu_us-_data_privacy_framework/> accessed 11 December 2023.

[127] Available at https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf. Accessed 14 December 2023.

[128] Available at https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf. Accessed 14 December 2023.

[129] Guillermo Cervio Munoa Martin A Roth, Sofía Requejado, Juan Manuel, 'Multijurisdiction: Ibero-American Network for the Protection of Personal Data - Standard Contractual Clauses for the International Transfer of Personal Data' (www.globalcompliancenews.com, 23 October 2022) <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 December 2023. As of the present date, Peru, Uruguay, and Argentina have either given approval or issued recommendations regarding the utilization of the RIPD model clauses.

[130] Lee Matheson, 'Not-So-Standard Clauses - Examining Three Regional Contractual Frameworks for International Data Transfers' (2023) The Future of Privacy Forum (FPF). Available at https://fpf.org/wp-content/uploads/2023/03/FPF-SCC-Not-So-Standard-Clauses-Report-FINAL-single-pages-1.pdf. Accessed 13 December 2023. This model serves as a non-binding framework for Latin American national data protection regulators and policymakers, illustrating their collective approach to cross-border data transfer tools. It aims to aid regulators in crafting tools that help entities handling personal data fulfil the requirements of Article 36.1(c) of the Personal Data Protection Standards for the Ibero-American States, that allows data transfers via signed contractual clauses or similar instruments ensuring adequate guarantees. The model comprises two contract frameworks, detailed in the Implementation Guide's Annex: Module 1 for transfers between data controllers and Module 2 for transfers between data controllers and data processors.

[131] Dörte Wollrad et al., 'EU-MERCOSUR Trade Agreement - Analysis of Sectoral Impacts in Brazil' (2021) Friedrich-

border data flows likely collides with its approach of affording a high level of protection of personal data' as a fundamental right.[132] In this sense, the EU traditionally upholds the principle that 'the protection of personal data is non-negotiable'.[133] In line with this, the EU's approach is 'to promote its data protection values and facilitate data flows by encouraging convergence of legal systems'.[134] This implies convergence with the EU's level of data protection.

While Brazil is not engaged in significant trade agreements incorporating digital trade provisions, it has shifted its historical defensive stance to better align with the US digital trade agenda.[135] Given this, Brazil faces the challenge of reconciling the LGPD 'with an ever-increasing alignment with the interests of the United States'.[136]

At the multilateral level, the Brazilian approach to the Joint Statement Initiative (JSI) on Electronic Commerce, initiated during the WTO 11th Ministerial Conference in December 2017, is worth mentioning. This initiative aims to establish a legally enforceable agreement among its participants, covering conventional trade matters like trade facilitation alongside various digital policy issues such as cross-border data movement, data localisation, online consumer protection, privacy, and network neutrality.[137]

The JSI has reached a consensus on several policy matters related to enhancing e-commerce. These matters encompassed e-signatures, e-contracts, spam regulation, and paperless trading.[138] In 2023, negotiations on cross-border data flows faced difficulties, particularly concerning privacy and personal data protection. A partial deal was made on data flows and localisation, with various approaches and proposals under consideration. The latest text showed some agreement among the parties. Some members, led by Australia, Japan and Singapore, championed provisions that enable and promote the

Ebert-Stiftung. Available at https://library.fes.de/pdf-files/bueros/bruessel/17416.pdf. Accessed 14 December 2023.

[132] Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' (2020) 10 International Data Privacy Law 3, August 2020, 201–221.

[133] Communication COM(2017)7 of 10 January 2017 from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN

[134] Ibid.

[135] Data Privacy Brasil, 'The intersection between AI regulation in the South and digital trade clauses involving source code and algorithms. Recap of Session 43 of the WTO's 2023 Public Forum organized by Data Privacy Brasil and REBRIP' (www.dataprivacybr.org, 16 October 2023) <https://www.dataprivacybr.org/en/the-intersection-between-ai-regulation-in-the-south-and-digital-trade-clauses-involving-source-code-and-algorithms/> accessed 11 December 2023.

[136] Wollrad et al. (n 131).

[137] 'The WTO Joint Initiative on e-commerce' (www.dig.watch) <https://dig.watch/processes/wto-ecommerce> accessed 11 December 2023.

[138] Yasmin Ismail, 'Policy Analysis - Joint Statement Initiative on E-commerce at Crossroads for a "Substantial" Conclusion by MC13' (www.iisd.org, 17 July 2023) <https://www.iisd.org/articles/policy-analysis/joint-statement-initiative-electronic-commerce> accessed 11 December 2023.

flow of data,[139] with limited exceptions to "legitimate public policy objectives",[140] in line with the US's influence in Asia-Pacific regional trade agreements. However, additional proposals were discussed, such as the European Union's suggestion for an exception related to privacy and personal data protection and Nigeria's proposal for policy flexibility aimed at developing and least-developed countries.[141] China, for its part, presented its proposal regarding data flows, aligning with commitments made in the Regional Comprehensive Economic Partnership (RCEP), expressing support for certain controls over data flows and data localisation requirements.[142] China has defensive interests 'in preferring the localisation of servers and public security exceptions for the free flow of data'.[143] According to the textual proposals on cross-border data flows, Brazil appeared to align with China in the proposed text concerning cross-border transfers of electronic information, for example, to recognise that each Party "may have its own regulatory requirements concerning the transfer of information by electronic means".[144]

At the regional level, the MERCOSUR Agreement on Electronic Commerce, signed on April 29, 2021, is noteworthy. The agreement aims to create a safer environment for the development of e-commerce, benefiting both companies and consumers. It covers several key areas, including the adoption and maintenance of legal frameworks related to the protection of personal data, the free transfer of information by electronic means for commercial purposes, the prohibition of the requirement to install servers in its territory as a requirement for doing business, and the protection against unsolicited commercial messages.[145] Personal data protection is regulated explicitly under Article 6 of the Agreement,[146] mandating Parties to establish or uphold laws, rules, or administrative measures to protect the personal information of individuals engaged in e-commerce activities, considering global standards. While acknowledging that each Party may have specific requirements concerning electronic information transfer, they are obliged to permit the cross-border exchange of information for commercial purposes via electronic means. Exceptions are allowed if a Party aims to accomplish a valid public policy objective,

---

[139] 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) <https://www.meti.go.jp/press/2022/01/20230120002/20230120002-3.pdf> accessed 10 February 2024.

[140] Ismail (n 138).

[141] ibid.

[142] 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 December 2023.

[143] Stefan Pantekoek, Yvonne Bartmann and Hajo Lanz, 'China's Role in the Multilateral Trading System' (2022) Friedrich-Ebert-Stiftung. Available at https://asia.fes.de/fileadmin/user_upload/documents/220517_China_Trading_System_EN_long_final_online.pdf. Accessed 14 December 2023.

[144] Section D.1 paragraph 4 of the WTO Electronic Commerce Updated Consolidated Negotiating Text – August 2023. Available at https://www.bilaterals.org/?wto-2023-plurilateral-ecommerce-48862. Accessed 12 December 2023.

[145] 'Press Release N. 50 - Signing of the MERCOSUR Electronic Commerce Agreement - Joint Press Release by the Ministries of Foreign Affairs and of Economy' (www.gov.br, 30 April 2021) <https://www.gov.br/mre/en/contact-us/press-area/press-releases/signing-of-the-mercosur-electronic-commerce-agreement-joint-press-release-by-the-ministries-of-foreign-affairs-and-of-economy> accessed 14 December 2023.

[146] Available at https://www.mercosur.int/documento/acuerdo-sobre-comercio-electronico-del-mercosur. Accessed 14 December 2023.

provided the measure is not arbitrary or unjustifiable, or a covert trade barrier.[147] Article 8 allows Parties to establish regulations concerning computer facilities, particularly to guarantee the security and privacy of communications. This section also addresses the concept of territoriality, explicitly prohibiting the imposition of a necessity to locate computer facilities within a specific territory as a condition for conducting business. However, there is a recognition that this prohibition might hinder governments from pursuing valid public policy goals. Therefore, despite the clear ban, Parties can impose territoriality requirements as long as these are grounded in legitimate reasons.[148]

After two decades of talks, the EU and the MERCOSUR states reached a political agreement on 28 June 2019 for a balanced and comprehensive trade agreement.[149] However, the deal is not final yet, as both blocs still need to settle some terms.[150] It is mentioned that the talks were delayed by the EU's insistence on more environmental safeguards, which prompted Brazil and Argentina to ask for more concessions.[151] The possible trade agreement would include, in the Chapter on Trade of Services, provisions on electronic commerce related to unsolicited marketing communications and consumer protection. 'Concerning electronic commerce and personal data protection, the agreement only addresses the prohibition of unsolicited or direct marketing'.[152] Additionally, Article 54, on General Exceptions, states that nothing in the chapter 'shall be construed to prevent the adoption or enforcement by either Party of measures: [...] (f) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to [...] (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'.[153]

Finally, the Brazil-Chile Free Trade Agreement (FTA) signed in November 2018 included commitments regarding the protection of personal information transferred across borders. This agreement specifically aimed at promoting regulatory alignment to ensure consistent levels of personal data protection. Chapter 10 of the Chile-Brazil FTA, on Electronic Commerce, acknowledges the importance of safeguarding the

[147] Celia Lerman, Gabriela Szlak and Lucía Suyai Mendiberri, 'MERCOSUR Electronic Commerce agreement: Challenges and opportunities' (2022) ADC (Association for Civil Rights) and Digital Trade Alliance. Available at https://adc.org.ar/wp-content/uploads/2022/09/MERCOSUR-ElectronicCommerceAgreement_ChallengesAndOpportunities-1.pdf. Accessed 14 December 2023.
[148] ibid.
[149] 'Press Release - EU and Mercosur Reach Agreement on Trade' (www.ec.europa.eu, 28 June 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_3396> accessed 14 December 2023.
[150] Kate Abnett, 'EU: conditions to complete Mercosur trade deal not met yet' (www.reuters.com, 7 February 2024) <https://www.reuters.com/world/europe/eu-conditions-complete-mercosur-trade-deal-not-met-yet-2024-02-07/> accessed 18 February 2024.
[151] 'Brazil's Lula Wants to Reach Mercosur-EU Deal This Year' (www.reuters.com, 21 November 2023) <https://www.reuters.com/world/americas/brazils-lula-wants-reach-mercosur-eu-deal-this-year-2023-11-21/> accessed 14 December 2023.
[152] Lerman et al. (n 147).
[153] Text available at http://www.sice.oas.org/tpd/mer_eu/Texts/Services_Establishment_e.pdf. Accessed 14 December 2023.

"right to the protection of personal data" for users engaged in electronic commerce (Article 10.2.5(f)).[154]

5. Conclusions

Brazil's digital prominence is not just a local phenomenon but a global one. As Latin America's largest e-commerce market and a key hub for data centres, Brazil's influence extends far beyond its borders.

In response to the need for comprehensive data protection regulations, Brazil enacted the LGPD in September 2020. The EU GDPR served as a model for the LGPD, and both laws have many common features. While sharing core aspects with the European regulation, the LGPD also incorporates distinct features tailored to Brazil's cultural and legal contexts, exemplified by specific provisions like credit protection, indicating potential flexibility in its application.

The LGPD is the cornerstone of Brazil's data protection framework, presenting a wide-ranging material scope and establishing a comprehensive set of data processing principles, rights and obligations. Following the GDPR's approach, the LGPD has a broad extraterritorial reach. The Brazilian Data Protection Authority, the ANPD, plays a crucial role ensuring compliance with LGPD provisions.

Chapter V of the LGPD regulates the cross-border transfer of personal data. These provisions allow personal data transfers if the destination country maintains an adequate level of protection, which the ANPD assesses. Furthermore, the LGPD allows international data transfers under specific circumstances. This includes scenarios where the data controller assures the safeguarding of personal data through distinct means: via transfer-specific contractual clauses; adherence to SCCs; compliance with binding corporate rules; or through seals, certificates and codes of conduct regularly issued. In addition, cross-border transfers are permitted when: it is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities; it is authorised by the ANPD; it is necessary for public policies or public service activities; data subjects have provided specific and highlighted consent for the transfer upon prior information; it is necessary for the fulfilment of a legal or regulatory obligation on the part of the controller; it is for a contract or procedures related to a contract in which the data subject is a party, as required by the data subject himself; and it is for the regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

ANPD released on August 15, 2023, a draft regulation on data transfers, which sets the requirements and guarantees for personal data exports, defines the content of SCCs, outlines the analysis process for specific contractual clauses and binding corporate rules, and specifies the adequacy decision assessment process for the data protection equivalence of foreign countries or international organisations. The draft outlines procedures for ANPD's recognition of equivalence for standard contractual clauses from other countries or international organisations (a process that may be initiated ex officio or upon the request of the

[154] It should be noted that '[w]hile many FTAs are quite benign to privacy, others may be toxic to domestic privacy laws which impose restrictions on cross-border data transfers' (Graham Greenleaf, 'Looming Free Trade Agreements Pose Threats to Privacy' (2018) 152 Privacy Laws & Business International Report, 23-27, UNSW Law Research Paper No. 18-38).

interested parties), emphasising approval prioritisation for widely applicable clauses. It also proposes a template for SCCs.

Brazil is currently seeking mutual adequacy recognition from the European Commission. The country has also expressed interest in potentially joining Convention 108+. As Brazil engages in ongoing trade negotiations and participates in multilateral forums like the WTO, it faces challenges reconciling its LGPD with multiple digital trade interests.

It can be argued that SSCs are key instruments for ensuring compliance with the Brazilian data protection framework when transferring personal data internationally. SSCs ensure further harmonisation of data protection obligations of data exporters and importers, regardless of the adequacy status of the destination country. The ANPD draft regulation on data transfers highlights the importance of SSCs in enhancing data transfer mechanisms, as well as the ANPD's role in assessing and approving them, reinforcing accountability measures for all parties involved in the data transfer process.

To foster convergence of data protection standards, aligning Brazilian SSC models, as much as possible, with the RIPD's SCCs approach could be beneficial. Moreover, if Brazil joins Convention 108+, it should also ensure compatibility with the Committee of Convention 108 Model Contractual Clauses for transborder data flows of personal data.

Brazil could also proactively promote the use of SSCs internationally as a mechanism that fosters interoperability between different legal frameworks for protecting privacy and personal data. This could include adopting and mutually recognising, where appropriate, similar SSCs that adhere to high personal data protection standards.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

COUNTRY DEEP DIVE 2: INDIA

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

Executive Summary

This policy report has been prepared within the framework of CERRE's flagship project on "Global Governance for the Digital Ecosystems" (GGDE). It is in line with the project's overarching goal: contribute to preserving and promoting regulatory convergence at the global level and, where convergence is neither desirable nor legitimate, to organizing co-existence. It is the second of a series examining how to achieve these objectives in the case of cross-border data flows, with a country deep dive on the mechanisms to achieve cross-border data flows in the context of India.

Following a long-drawn deliberation process, India recently adopted its first comprehensive data protection law in 2023. The Digital Personal Data Protection Act, 2023 (DPD Act, 2023), which is expected to come into effect during this year, differs from other global data protection frameworks in some respects. For instance, it applies only to data that is collected or processed in a digital form, it does not create a separate category of sensitive personal data and does not entitle individuals to seek compensation from data fiduciaries for any harms caused to them. Further, the law is also silent on some of the other aspects that are seen in laws like the European GDPR. For instance, the rights related to data portability, the right to be forgotten, and automated decision-making. However, the government has indicated that some of these aspects may be covered under a future companion legislation to the DPD Act, known as the proposed Digital India Act.

The treatment of cross-border data flows is another point of divergence. The position adopted by the Indian law is that personal data will be allowed to flow freely, except to a set of restricted countries that can be notified by the government. This represents a significant shift from the initial drafts of the law, which proposed strict localisation requirements for certain types of data and identified mechanisms like adequacy assessments, model contract clauses and intra-group schemes as conditional modes of data transfers.

While the new law has settled on a fairly liberal stance toward personal data flows, it leaves the door open for the adoption of more stringent restrictions under other laws. India already has a number of such sector/ data-type related transfer restrictions that are applicable to the financial sector, telecommunication and broadcasting services, corporate and compliance requirements, and government data.

Set against this background, Section 1 of the paper begins with a discussion on India's key data governance initiatives and priorities, much of which has been centred around the role of data for effective governance, innovation and empowerment. It highlights the role of digital public infrastructure solutions like the Data Empowerment and Protection Architecture and the proposed National Data Management Office in the country's data governance strategy.

Section 2 describes the evolution of India's data protection framework, with a focus on the scope, rights and obligations and enforcement mechanisms under the DPD Act, 2023. This is followed, in Section 3, with a deep dive into the cross-border flow related provisions. The section describes the transition from the localisation recommendations of 2018 to the blacklisting approach under the DPD Act. It then maps

out the different sector-specific restrictions that exist in India and explores the country's position on data sharing and data flows under international arrangements.

Section 4 presents an analysis of the key issues that emerge from the discussions and offers some recommendations. Rather than making broader suggestions on general improvements that may be needed to the DPD Act, the paper limits itself to recommendations on issues related to cross border data flow.

First, it recommends that, in order to minimize fragmentation and uncertainty, the law should set out the basic principles, criteria, and processes to govern the adoption of any sectoral data flow restrictions. The government's power to impose restrictions on data flows to specific countries should also be bound by such reasonable and identified criteria.

Second, it suggests that stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses that would meet the requirements of the DPD Act, and ideally go beyond that, through an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.

Third, the paper makes a case for legislative reforms to strengthen the country's surveillance and law enforcement framework. Besides being violative of citizens' privacy rights, unchecked powers of law enforcement and intelligence agencies are also detrimental to the free flow of data into the country. The suggested reforms would include the introduction of requirements of judicial approval for interception requests, notice to individuals, data minimisation requirements, and suitable redress mechanisms.

1. Context

With a population of over 1.4 billion India is now the most populous country in the world.[1] It is the fifth largest economy globally, based on Gross Domestic Product (GDP)[2]. As a lower-middle income country with a rapidly growing economy, India also straddles multiple trade and strategic relationships. It counts the United States (US), China, and the United Arab Emirates (UAE) among its largest trading partners.[3] The country is also known for its leadership in information technology (IT) and business process management services. It holds over fifty percent of the global outsourcing market, with the US, the European Union and

[1] Laura Silver, Chrustine Huang and Laura Clancy, Key facts as India surpasses China as the world's most populous country, Pew Research (9 February 2023) <https://www.pewresearch.org/short-reads/2023/02/09/key-facts-as-india-surpasses-china-as-the-worlds-most-populous-country/>.

[2] World Bank national accounts data (2022) <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true>.

[3] World Integrated Trade Solution, Top 5 Import and Export Partners (2021) <https://wits.worldbank.org/CountryProfile/en/Country/IND/Year/2021/Summary>. Also see Fazal Rahim, India's foreign trade in 2023: Its top trading partners and most traded commodities, Forbes India (29 December 2023) <https://www.forbesindia.com/article/news/indias-foreign-trade-in-2023-its-top-trading-partners-and-most-traded-commodities/90611/1>.

the United Kingdom as its largest importers.[4]

In terms of intergovernmental partnerships, India is a member of the Group of Twenty (G20) alliance among the world's largest economies, the Quad diplomatic partnership with Australia, Japan, and the United States, and is recognized as a key partner by the OECD. At the same time, it also prioritizes south-south collaborations through forums like the BRICS forum and the Group of 77 alliance of developing countries.

Despite persisting digital divides, India hosts the world's second largest Internet user base of more than 890 million Internet subscriptions.[5] The foundation of India's digital society rests on the strength of this digital population. Bringing more people online and encouraging their adoption of digital goods and services has, therefore, been a focus for the government and the private sector alike. Correspondingly, the commercial and developmental value of the data generated from such digital interactions has also been in the spotlight.

A large part of the data-related discourse in India is powered by the idea of data being a valuable resource that needs to be harnessed to meet the country's economic and developmental objectives. This includes highlighting the role of data for effective governance and innovation and as a source of citizen empowerment.[6] For instance, India's Economic Survey of 2018-2019 contained a chapter on "Data 'Of the People, By the People, For the People'".[7] The report focused on the different types of data that the government holds about citizens –administrative, survey, institutional and transactions data– and the need to streamline, interlink and unlock this data for public good. Researchers have also identified the role of the government as a market architect and the narrative around countering 'data colonialism' as some of the other drivers behind India's data governance strategy.[8]

The country's reliance on digital public infrastructure (DPI), as the predominant path to digital transformation,[9] has also influenced its data governance solutions. Two examples of such data governance-centric DPIs, which emphasize the importance of digital infrastructures for improved data

---

[4] India Brand Equity Foundation, Servies: Services exports from India stood at US$ 322.72 million in FY23 (November 2023) <https://www.ibef.org/exports/services-industry-india>.

[5] Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators April–June, 2023' (5 December, 2023) <https://www.trai.gov.in/sites/default/files/QPIR_05122023_0.pdf> accessed 29 January 2024.

[6] Ministry of Electronics and Information Technology, National Data Governance Framework Policy (Draft) (May 2022) <https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf>.

[7] Economic Survey of 2018-2019, Data "Of the People, By the People, For the People" <https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf>

[8] Neha Mishra, Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?, in Data Sovereignty: From the Digital Silk Road to the Return of the State, Anupam Chander and Haochen Sun (eds.) (New York, 2023; online edn, Oxford Academic, 14 December 2023) <https://doi.org/10.1093/oso/9780197582794.003.0011>.

[9] Smriti Parsheera, Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process, 52 Computer Law & Security Review (April 2024) <https://doi.org/10.1016/j.clsr.2024.105947>.

gathering, storage, processing and dissemination, are currently in motion. The first, the Data Empowerment and Protection Architecture (DEPA), is a technical architecture designed to facilitate the sharing of personal data among entities, relying on an electronic consent artifact.[10] This artifact would record the individual's consent for the sharing of their data held by one entity, such as a diagnostic lab, with another entity, such as a hospital. In the financial sector, DEPA has been implemented under the regulatory framework governing a new category of intermediaries called 'account aggregators'.[11] These entities act on the user's consent to facilitate the flow of encrypted information among financial institutions through the use of application programming interfaces (APIs).

The second initiative relates to the move toward the creation of a 'India Data Management Office' (IDMO) that was introduced in the draft National Data Governance Framework Policy released in 2022.[12] The proposed IDMO will be responsible for developing rules and standards to govern the collection, management and exchange of non-personal and anonymized data generated by government entities. Private entities would also be encouraged to contribute to its dataset's generation program and a subset of them (specifically, only India-based entities) would also be allowed access to the datasets. The final version of this policy is yet to be notified.[13]

Besides such technical architectures for data management, India has launched a number of policy deliberations pertaining to data governance. Notable among these are the enactment of the Digital Personal Data Protection Act, 2023 (DPD Act), which is discussed further in Section 2, and a proposal for the regulation and sharing of non-personal data. In 2019, the Indian government set up a committee of experts on non-personal data. The committee recommended the need for a new regulatory framework for unlocking the economic benefit of non-personal data that is generated in India and should be available to meet the country' governance and innovation goals.[14] Unlike the IDMO initiative, which concentrates primarily on government-owned data, the committee recommended that even private businesses should be compelled to create and share 'high value datasets' for certain public good purposes.[15] The government is yet to take a final decision on the committee's recommendations although the proposed IDMO might be a precursor to such a move.

The issue of cross border data flows has featured prominently in many of these regulatory discussions. Notably so, in the case of the data protection law, which went through many draft versions until its final

[10] NITI Aayog, 'Data Empowerment and Protection Architecture: Draft for Discussion' (2020) <https://www.niti.gov.in/sites/default/ files/2020-09/DEPA-Book.pdf>; Draft Report by the Committee of Experts on Non-Personal Data Governance Framework (16 December 2020) <https://static.mygov.in/static/s3fs-public/mygov_160975438978977151.pdf> accessed 2 February 2024.

[11] Press Information Bureau, Know all about Account Aggregator Network – A financial data-sharing system (September 2021) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713>.

[12] Ministry of Electronics and Information Technology (n 6).

[13] Gargi Sarkar, Draft National Data Governance Policy Under Finalisation: Centre, Inc42 (1 February 2024) <https://inc42.com/buzz/draft-national-data-governance-policy-under-finalisation-centre/>.

[14] Committee of Experts on Non-Personal Data Governance Framework (n 10).

[15] The indicated list of public purposes would include improving public services, agriculture, healthcare, job creation, poverty alleviation and financial inclusion.

enactment in 2023. These draft versions of the text contained varying levels of data flow restrictions, starting from the proposal for mandatory mirroring of all personal data on Indian servers in the first draft of 2018 to the significantly relaxed approach adopted in the enacted version. Section 3 of the paper describes the progression of these ideas as well as the interplay between the data protection law and various sector-specific data flow restrictions that will continue to remain in effect.

The Indian government is in the process of formulating another law, the proposed Digital India Act, which it describes as a 'companion legislation' to the DPD Act.[16] While a draft of this has not yet been published, an early consultation document indicates that the proposed law will cover various aspects of digital user rights, including the right to be forgotten, right to redress, and right against discrimination and automated decision making.[17] The manner in which the provisions of the DPD Act will interact with the proposed Digital India Act is not yet clear.

At present, India is not pursuing an independent legislation to regulate artificial intelligence, although some aspects of this will be covered under the Digital India Act. Its official think tank, the NITI Aayog has, however, formulated a national AI strategy document[18] and the government has issued various advisories on the subject. For instance, the advisory directed at significant social media intermediaries to identify misinformation and deepfakes.[19] More recently, the government introduced, and then hastily backtracked on, another controversial advisory that advised the need for taking its permission before deploying 'unreliable' AI models.[20]

2. Legal framework on data protection

India is a recent entrant into the club of jurisdictions with comprehensive data protection laws. Its DPD Act was approved by both houses of the Parliament and received the President's assent in August 2023. The new law is, however, yet to come into effect. The Ministry of Electronics and Information Technology (MeitY), the ministry in charge of this subject, is likely to start notifying different provisions post the conclusion of India's general elections in June 2024.[21] Meanwhile, the MeitY is reported to be in the

[16] Ministry of Electronics and Information Technology, Digital Personal Data Protection Act is a world-class legislation: MoS Rajeev Chandrasekhar (13 August 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357>.

[17] Ministry of Electronics and Information Technology, Proposed Digital India Act, 2023, Digital India Dialogues (9 March 2023) <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf>.

[18] NITI Aayog, National Strategy for Artificial Intelligence (June 2018) <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>.

[19] Ministry of Electronics and Information Technology, Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes (7 November 2023) <https://pib.gov.in/PressReleasePage.aspx?PRID=1975445>.

[20] Amber Sinha, The Many Questions About India's New AI Advisory, Tech Policy Press (6 March 2024) <https://www.techpolicy.press/the-many-questions-about-indias-new-ai-advisory/>; Paritosh Chauhan, Sameer Avasarala and Abhishek Singh, MEITY Advisory: Dawn of AI Regulation in India or a false start, Lexology (1 April 2024) <https://www.lexology.com/library/detail.aspx?g=47dda3b5-1111-4b6b-9f87-799ef8066802>.

[21] Ashmit Kumar, Data Protection Framework postponed until after Lok Sabha elections: Sources, CNBC TV18 (17 January 2024) <https://www.cnbctv18.com/technology/data-protection-framework-postponed-dpdp-notifcation-

process of developing the draft rules needed to operationalize various aspects of the new law.[22]

Until the DPD Act is brought into effect, data protection issues continue to be governed mainly under the limited set of protections offered under Section 43A and 72A of the Information Technology Act, 2000. Section 43A of this law provides for compensation in case a body corporate fails to maintain reasonable security practices while dealing with sensitive personal data. Section 72A lays down criminal penalties for unauthorized disclosure of personal data. The government has also framed a set of rules governing the processing and security of sensitive personal data under Section 43A.[23] Among other provisions, the rules lay down requirements related to data transfers, providing that a transfer should be made only if it is necessary for the performance of a lawful contract or with the individual's consent.[24] Further, the parties to the transfer will be bound to ensure that the data remains subject to the same level of data protection as set out under the rules for the body corporate collecting the data.[25] Upon the implementation of the DPD Act, the data flow conditions under these rules will be replaced by the relatively less restrictive framework for cross-border data flows under the new law.

2.1. Evolution of the data protection law

Policy discussions on the need for a standalone privacy law had been going on in India since 2010,[26] but the process did not see much traction until a few years ago. In August 2017, a nine-judge bench of the Supreme Court examined the issue of whether the Indian Constitution guarantees a fundamental right to privacy. Answering the question in the affirmative, the court in Justice KS Puttaswamy and another v. Union of India[27] laid down that privacy is a fundamental right, although not an absolute one. The judges held that any reasonable intrusion into the right to privacy would be valid only if it satisfies the tests of legality, legitimate aim, and proportionality. Such an intervention must also incorporate reasonable procedural safeguards.[28]

---

after-lok-sabha-elections-18823331.htm>.

[22] Aditi Agrawal, Draft rules on data protection to be shared this week: MoS Chandrasekhar, The Hindustan Times (21 December 2023) <https://www.hindustantimes.com/india-news/draft-rules-on-data-protection-to-be-shared-this-week-mos-chandrasekhar-101703159717469.html>.

[23] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 <https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>.

[24] Rule 7, Information Technology Rules, 2011.

[25] This includes requirements relating to maintaining reasonable security practices and not retaining the information for longer than is required for the original, lawful, purpose.

[26] Ministry of Personnel, Approach paper for a legislation on privacy (Draft) (13 October 2010) <https://documents.doptcirculars.nic.in/D2/D02rti/aproach_paper.pdf>. Also see Malavika Raghavan, Are we there yet? The long road to nowhere: The demise of India's draft data protection bill, Future of Privacy Forum (October 2022) <https://fpf.org/blog/are-we-there-yet-the-long-road-to-nowhere-the-demise-of-indias-draft-data-protection-bill/>.

[27] Justice KS Puttaswamy and another v. Union of India, Writ Petition (Civil) No. 494 of 2012 <https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf>

[28] Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, An analysis of Puttaswamy: the Supreme Court's privacy verdict, The LEAP Blog (20 September 2017) <https://blog.theleapjournal.org/2017/09/an-analysis-of-

Further, a plurality of the judges in the Puttaswamy decision recognized that the right to privacy consists of many different facets, informational privacy being one of them. They observed that data protection is a complex exercise which needs to be undertaken by the state after a careful balancing of the requirements of privacy coupled with other values and the state's legitimate concerns.[29] In the lead up to this verdict, the Indian government set up an expert committee to study the issues relating to data protection in India and recommend a draft data protection bill. The committee, headed by a former Supreme Court judge, Justice B.N. Srikrishna, identified the need to develop a legal framework that would speak to India's priorities as a developing nation while also drawing upon the best practices of data protection in more developed democracies.[30] As per several accounts, the committee's Draft Data Protection Bill of 2018[31] ended up drawing significant inspiration from the European General Data Protection Regulation (GDPR). Yet, it also left room for improvements in order to be better tuned to the Indian context.[32]

Following public consultations, the MeitY generated a revised version of the bill, which was introduced in Parliament as the Personal Data Protection Bill of 2019.[33] A Joint Parliamentary Committee (JPC), consisting of members from both houses of the Indian Parliament, was then tasked to review the bill and offer their recommendations on it. The JPC recommended that the scope of the bill should explicitly cover both personal and non-personal data, including anonymized personal data.[34] The committee also suggested other edits to increase the scope of harms under the law, impose stricter regulations on social media intermediaries, and regulate data-collecting hardware manufacturers. However, in 2022, the government announced its decision to withdraw the pending bill and subsequently replaced it with a new draft. This revised draft of 2022 is the one that eventually made it to the rule book as the DPD Act.

2.2. Scope of the DPD Act

puttaswamy-supreme.html#gsc.tab=0>.

[29] Chandrachud J. in Justice KS Puttaswamy and another v. Union of India, para 179, p. 253.

[30] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Ministry of Information Technology and Electronics (July 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 30 January 2024.

[31] The Personal Data Protection Bill, 2018 <https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

[32] Nilesh Christopher, Srikrishna Committee Report: Draft bill gets mixed response from experts, The Economic Times (28 July 2018) <https://economictimes.indiatimes.com/news/politics-and-nation/srikrishna-committee-report-draft-bill-gets-mixed-response-from-experts/articleshow/65171992.cms?from=mdr>; Raman Jit Singh Chima, Naman M. Aggarwal and Akash Singh, India's Draft Data Protection Bill Needs to do More to Stack Up Against Global Standards, The Wire (25 September 2018) <https://thewire.in/tech/data-protection-bill-supreme-court-puttaswamy-judgment>.

[33] The Personal Data Protection Bill, 2019 <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>

[34] Report of the Joint Committee on Personal Data Protection Bill, 2019, Lok Sabha Secretariat (2021) <https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf>.

The DPD Act will govern the processing of all digital personal data – data that is collected in a digital form or digitized post collection– that takes place in India. It will also have extraterritorial scope over processing that takes place outside India but is connected with a business or systematic activity of offering goods or services to, or the profiling of, persons in India.[35] In terms of nomenclature, starting from Justice Srikrishna committee's draft bill in 2018, India has used the terms 'data principal' and 'data fiduciary' to identify what the European GDPR would call the 'data subject' and 'data controller'. In the committee's view, the term principal was better suited to capture the individual's role as 'the focal actor in the digital economy' while the concept of fiduciary was invoked to imply a duty of care to deal with the individual's data fairly and responsibly.[36] Researchers observed that the scope of duties and the standards laid down in the committee's draft law, which have only been diluted over time, were not as high as seen in cases of traditional fiduciary relationships like doctor-patient and lawyer-client.[37] But it remains to be seen if the implementation of the DPD Act could result in the development of a new body specific to the processing of personal data.[38]Next, the law contains several exclusions and exemptions from its scope. To begin with, the DPD Act will not apply to any processing done by an individual for personal or domestic purposes. Any data that is made publicly available by the relevant data principal, such as on social media, or by any other person under a legal obligation is also excluded.[39] Further, the law also excludes any processing done for research, archiving or statistical purposes so long as no specific decision is being made about the data principal and such processing adhered with prescribed standards.[40] The scope of what is covered under the meaning of 'research' has not been laid down in the law and will likely be clarified in the standards to be prescribed by the government for this purpose.

Further, there are two other categories of exemptions. The first relates to exemptions from an albeit broad, but identified, set of provisions for purposes like judicial or regulatory, law enforcement, giving effect to a merger or amalgamation, and default in loan payment.[41] The second group covers those cases where the power to notify the exemption is vested in the hands of the government. For instance, the power to exempt state instrumentalities for national interest or public order objectives or Indian startups and other select fiduciaries to ease their compliance burden.[42] In addition, there is an open-ended power for the government to declare, within the first five years, that any provision of the law will not apply to any fiduciary(ies) for a notified period.[43]

---

[35] Section 3(a) and (b), DPD Act 2023.
[36] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 30), p. 8.
[37] Rishab Bailey and Trishee Goyal, Fiduciary Relationships as a Means to Protect Privacy: Examining the Use of the Fiduciary Concept in the Draft Personal Data Protection Bill, 2019' (The Leap Blog, 13 January 2020) <https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html>
[38] Smitha Krishna Prasad, Information Fiduciaries and India's Data Protection Law, Data Catalyst (September 2019) <https://datacatalyst.org/wp-content/uploads/2020/06/Information-Fiduciaries-and-Indias-Data-Protection-Law.pdf>.
[39] Section 3(c), DPD Act 2023.
[40] Section 17(2)(b), DPD Act 2023.
[41] Section 17(1), DPD Act 2023.
[42] Section 17(2)(a) and 17(3), DPD Act 2023.
[43] Section 17(5), DPD Act 2023.

2.3. Rights and obligations

The processing of personal data can take place either based on the consent of the data principal or under any of the specified 'legitimate uses'. The list of legitimate grounds includes voluntary provision of data to the data fiduciary, which is not accompanied by a denial of consent for its processing, provision of services and benefits by the state, disasters and medical emergencies.[44] Further, data processing for employment-related purposes and to protect the employer from incidents of corporate espionage or intellectual property breach is also classified as a legitimate use.

In situations where the data processing is based on consent, the law provides for a requirement of notice about the purpose of the processing and the manner in which the individual can exercise their rights. Taking into account the diversity of the Indian population, the law requires that the individual should be given the option to access any request for in English or any of the twenty two Indian languages specified in the Constitution.[45] However, unlike many other data protection laws, the DPD Act does not recognize a separate category of sensitive personal data that may merit higher safeguards for notice and consent or for any other purposes. This also stands in contrast with the position under IT Act and rules, which applied specifically to sensitive personal data.

There is a list of general obligations that have been cast on data fiduciaries.[46] This includes ensuring the completeness and accuracy of data, reasonable security safeguards to prevent a data breach, erasure of personal data, and an effective mechanism for grievance redress. Further, the processing of children's data is subject to requirements of verifiable parental consent and restrictions on tracking, behavioural monitoring and targeted advertising aimed at children.[47] In addition to these general requirements, an additional set of obligations, including conduct of impact assessments and external data audits, will apply only to 'significant data fiduciaries' to be notified by the government.[48]

The DPD Act also grants four categories of rights to data principals. In case of consent based processing, the person is entitled to seek a summary of their processed data and identities of others with whom the data has been shared.[49] Similarly, the right to correction and erasure of data is also limited to consensual processing.[50] The two other rights – that of access to grievance redress and the right to appoint a nominee to deal with a person's data upon their death or incapacity – will apply in all cases.[51] While conferring these rights, the law casts a set of expected duties from the data principal, such as not suppressing any material information and not filing false or frivolous complaints.[52]

---

[44] Section 7, DPD Act.
[45] Sections 5 and 6, DPD Act 2023.
[46] Section 8, DPD Act 2023.
[47] Section 9, DPD Act 2023.
[48] Section 10, DPD Act 2023.
[49] Section 11, DPD Act 2023
[50] Section 12, DPD Act 2023.
[51] Section 13 and 14, DPD Act, 2023.
[52] Section 15, DPD Act 2023.

2.4. Enforcement framework

The DPD Act provides for the creation of a new statutory body called the Data Protection Board of India (the Board) to inquire into compliance with the provisions of the law. The Board's functions will also include directing remedial or mitigation measures against any data breach, checking compliance by consent management intermediaries registered under the DPD Act.[53] While the text of the law states that the Board will function as an independent body,[54] commentators have called into question the extent of this independence in light of the significant government control over the membership and functioning of the Board.[55]

Pursuant to conducting an inquiry, the Board may impose monetary penalties up to the limits specified in the law for different types of actions. While doing so, it should take into account facts like the nature and gravity of the breach, its repetitive nature and existence of any mitigating actions. The maximum penalty specified in the Schedule stands at Indian Rupees 2.5 billion (approximately 27.5 million Euros). An appeal against the order of the Board can be made to an Appellate Tribunal designated under the law. Notably, there is no provision for the payment of compensation to data principals for harms caused to them by a data fiduciary or processor. This is unlike the provisions seen in laws like the GDPR or the right to compensation under Section 43A of the IT Act, which will no longer remain in effect.

Departing from earlier drafts of the bill, the DPD Act also does not confer any regulation-making powers on the Board.[56] It, however, identifies several areas for rulemaking by the central government. The list of powers in Section 40 includes the manner of issuance of notice, exemptions related to processing of children's data, and the process of conducting data protection impact assessments. In addition, the government also has the power to issue notifications on several important subjects, including cross border data flows, which is discussed in the next section. Further, the government can, based on a reference received from the Board, issue directions for the blocking of the business activities of an entity upon which a monetary penalty has already been imposed in two or more instances.[57]

2.5. Data access for surveillance and law enforcement

The broad exemptions afforded by the DPD Act for law enforcement and other designated purposes come against the background of a deficient framework of surveillance-related protections under other laws.[58]

---

[53] Section 27, DPD Act 2023.
[54] Section 28, DPD Act 2023.
[55] Aarathi Ganesan, Will the Composition of the Data Protection Board of India Impact How it Handles Data Privacy Complaints?, Medianama (2 November 2023) <https://www.medianama.com/2023/11/223-composition-data-protection-board-impact/>; Gargi Sarkar, Experts Raise Questions On The Autonomy Of The Proposed Data Protection Board, Inc42 (
25 November 2022 <https://inc42.com/buzz/autonomy-of-the-proposed-data-protection-board-is-in-question-experts/>.
[56] Anirudh Burman, Understanding India's New Data Protection Law, Carnegie India (3 October 2023) <https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624>.
[57] Section 37, DPD Act 2023.
[58] Jhalak M. Kakkar et al, The Surveillance Law Landscape in India and The Impact of Puttaswamy, National Law

The interception of telecommunications messages and information on a computer resource is governed by Section 69 of the Information Technology Act, 2000 and Section 20(2) of the Telecommunications Act 2023 (previously Section 5(2) of the Telegraph Act, 1885). These provisions allow for the government to call for the interception and disclosures of messages to the government on grounds such as the sovereignty and integrity of the nation, defence and state security, public order, or preventing the incitement of any offense.

Following a Supreme Court decision in 1997,[59] the government adopted a set of rules, which were outlined by the court, to govern its interception procedures.[60] The rules designate a senior government official as the person authorized to issue interception orders. However, such orders are not required to be sanctioned by a judicial authority. The only available form of oversight is in the form of a review committee, also consisting of members from the executive, that is supposed to meet at least every two months to review interception orders. There are a few other safeguards like the requirement that such orders should be issued 'only when it is not possible to acquire the information by any other reasonable means'[61] and a prohibition on the use or disclosure of the intercepted messages for any other purpose.[62]

The provisions, however, remain silent on other important aspects like independent oversight, notice to the affected person, and transparency and reporting obligations of law enforcement agencies.

Besides the provisions on lawful interception, access to personal data can also be obtained under other laws. Notably, Section 91 of the Code of Criminal Procedure, 1973 contains a broad power enabling an officer in charge of a police station to compel the production of 'any document or other thing' if that is 'necessary or desirable' for the purposes of an investigation. For instance, this power can potentially be used by the police to seek the call data records or SMS logs of an individual, although there have been a handful of cases where courts have stepped in to hold that a blanket request for call records would amount to an unjust invasion into the privacy of the individual.[63]

3. India's position on cross-border data flows

The treatment of cross-border data flows has been among one of the most contested aspects of the Indian data protection law. It is also an area that has undergone drastic shifts during the law's evolutionary

University Delhi, Centre for Communication Governance (June 2023) <https://globalnetworkinitiative.org/wp-content/uploads/2023/07/CCG-June-15.pdf>

[59] People's Union for Civil Liberties v Union of India (1997) 1 SCC 30.

[60] Rule 419A, Indian Telegraph Rules, 1951. Similar rules have also been adopted for interception of information on a computer resource under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[61] Rule 8, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[62] Rule 25(2), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[63] Tarun Krishnakumar, Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973, 15 Indian Journal of Law and Technology (2019) 67, at p. 87 to 89.

process. In 2018, the Justice Srikrishna Committee came up with a fairly stringent set of data localisation norms. They identified improving law enforcement, safeguarding against threats to disruption of critical infrastructure, building artificial intelligence systems in India, and preventing foreign surveillance as the key advantages of data flow restrictions.[64]

At that point, the draft law provided for different classes of personal data and the committee recommended that at least one serving copy of all personal data should be kept on a server located in India. Further, certain categories of critical personal data, that were to be determined by the government, were to be processed exclusively in India. The committee also suggested that any data flows would be subject to requirements like permissible transferee countries designated by the government, standard contractual clauses or intra-group schemes approved by the data protection authority, and consent from the individual.

Following significant pushback from a cross-section of stakeholders, the 2019 version of the bill saw a comparatively diluted version of these proposals. It did away with the data mirroring requirement for all types of personal data. It, however, maintained such a provision in respect of sensitive personal data while retaining the requirement that critical personal data would be processed only in India. Subsequently, the JPC also echoed its support for having such restrictions in the law.

As per the JPC, the motivations for localisation included national security and law enforcement interests, better informational privacy, employment generation and other economic benefits, and strengthening India's bargaining powers in international interactions.[65] In addition, the JPC suggested tightening the draft provisions on conditional transfers in a few ways. For instance, they proposed that transfers based on a contract or intra-group scheme should not be approved if such an instrument goes against public policy or the state policy of India. This was defined as situations where the instrument "promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizen".[66]

The 2022 version of the bill and the DPD Act, however, ended up doing a volte-face on the previous recommendations. The draft bill put out by MeitY in 2022 opted for what may be called a 'whitelisting' approach. It provided that the government would notify the countries to which data could be transferred and the terms and conditions for such transfer. While some saw this as a reversal of the localisation mandate, the provision could also be interpreted to mean that all data transfers would be prohibited, until specified otherwise by the government. In the end, the DPD Act of 2023 chose to replace this with a more liberal 'blacklisting' approach that is described below.

3.1. Data transfers under the DPD Act

Section 16 of the DPD Act provides that the government may notify specific countries or territories the

[64] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 21) p. 88-93.
[65] Report of the Joint Parliamentary Committee (n 34), p. 41.
[66] Report of the Joint Parliamentary Committee (n 34), p. 111-112.

transfer of personal data to which would be restricted. This effectively means that all transfers will be permitted, unless specified otherwise. In addition to the possibility of country-specific restrictions, the DPD Act also reserves space for other laws that may impose 'a higher degree of protection for or restriction on transfer of personal data'.[67] The law does not set out any grounds or criteria that the government must take into account while notifying the restricted destinations. However, it introduces some element of accountability in such decisions by providing that the notification will have to be placed before the Parliament to enable scrutiny and allow for its modification or cancellation by the Parliament.[68]

While the Indian law does not speak of the role of contractual arrangements or model clauses in the context of data transfers, it does contain general requirements relating to arrangements with data processors. As per Section 8(2), data fiduciaries can engage data processors to process personal data on their behalf only under a valid contract. The contents of such a contract have not been outlined in the law. Neither does it mandate the government to issue any rules or guidelines in this regard. The DPD Act, however, makes it clear that the data fiduciary would continue to remain fully responsible for compliance with the law in respect of any processing undertaken on its behalf by a processor. The Act also makes specific references to ensuring compliance by processors in a few contexts, like maintaining reasonable security safeguards to prevent personal data breach, erasure of data upon expiry of the retention period, and to cease processing the personal data of a data principal if they withdraw their consent.[69] Further, the data principal's right to information access includes information about the identities of all data processors with whom their data has been shared along with a description of the shared data.[70]

Therefore, even though not mandated by the law, there could be a role for the emergence of standard contractual clauses that are in line with the DPD Act to govern the relationship between data fiduciaries and processors. This could support the legal requirements of there being a valid contract between the data fiduciary and the data processor and the fiduciary remaining responsible for the activities of its processors.

Taking into account the interests of the Indian outsourcing and business processes management industry, the DPD Act also carves out an exception for such arrangements. It exempts the processing of data under a contract between a person outside India and a person based in India, as long as it does not relate to data principals in India, from a bulk of the provisions of the Act.[71] A provision of this nature could also be linked with the concept of 'data embassies' that was put out by the Indian Finance Minister in her 2023 budget speech.[72] Such data embassies could serve as corridors of trust through which governments, and possibly private actors too, would be able to locate their data in another jurisdiction without being subject to the local laws of that jurisdiction. India is yet to issue any policy directions on the mechanisms and legal

[67] Section 16(2), DPDP Act 2023.
[68] Section 41, DPDP Act 2023.
[69] Sections 8(5 and (7) and Section 6(6), DPDP Act 2023.
[70] Section 11(1)(b), DPDP Act 2023.
[71] Section 17(1)(d), DPDP Act 2023.
[72] The Economic Times (3 February 2023) <https://economictimes.indiatimes.com/tech/technology/govt-may-notify-data-embassy-policy-as-part-of-new-data-bill/articleshow/97560396.cms>.

framework governing this proposal.

Sector-specific restrictions

Although the DPD Act has settled on a fairly liberal position toward data transfers, India already sees a number of restrictions on data flows across sectors. Such restrictions, which are described further in the table below, can be grouped into the following four buckets: i) data pertaining to financial services, ii) data of telecommunications and broadcasting subscribers, iii) corporate and compliance data, and iv) government data.[73] The table below outlines these restrictions in detail, across the different buckets outlined above.

Category	Authority	Instrument	Provision
Financial services			
Payments data	Reserve Bank of India	Directive on Storage of Payment System data, 2018	All data related to payment transactions has to be stored on a system only in India. Limited exception for cross-border payments.
Insurance policyholder records	Insurance Regulatory and Development Authority of India	Outsourcing of Activities by Indian Insurers Regulations, 2017	Insurer to ensure compliance of local laws while outsourcing services. Original policyholder records need to be maintained in India, which implies that a transfer is possible subject to this condition.
Video KYC data	Reserve Bank of India	Master Direction on Know Your Customer, 2021	Data and recordings of customer KYC to be stored on systems located in India.
Telecommunication and broadcasting			
Telecommunication subscriber data	Department of Telecommunications	Unified License Agreement	Cannot transfer user's accounting information to persons/ place outside India.

[73] Smriti Parsheera, What's Shaping India's Policy on Cross-Border Data Flows? in Evan A. Feigenbaum and Michael R. Nelson (eds), *How India and Korea Can Drive New Thinking About Data*, Carnegie Endowment for International Peace (2022) <https://carnegieendowment.org/2022/08/31/what-s-shaping-india-s-policy-on-cross-border-data-flows-pub-87769>.

			Exception for international roaming
Broadcasting subscriber data	Department for Promotion of Industry and Internal Trade	Consolidated Foreign Direct Investment Policy, 2020	Cannot transfer subscribers' databases to any persons/place outside India unless permitted by law
Corporate and compliance			
Books of companies' accounts	Ministry of Corporate Affairs	Companies (Accounts) Rules, 2014	Back-up of the books of account must be kept on servers physically located in India
Risk and compliance data of financial institutions	Securities and Exchange Board of India	Advisory for Financial Sector Organisations	Institutions utilising software as a service must keep critical data relating to risk, audits, and compliance within India.
Logs of all ICT systems	Indian Computer Emergency Response Team (CERT-In)	Directions under Information Technology Act, 2000	Service providers, intermediaries, data centres, body corporate and government organisations need to keep ICT system records in India for a rolling period of 180 days.
Government data			
Public records	Parliament, National Archives of India, and the Ministry of Culture	Public Records Act, 1993	Cannot take public records out of India without prior approval of the central government, except if sent out of India for any official purpose
Cloud storage of government data	Ministry of Electronics and Information Technology	Guidelines on Contractual Terms for Cloud Services	Data centre facilities and the physical and virtual hardware should be located within India
Shareable data held by the Indian	Department of Science	National Data Sharing and	Open government data platform to be managed and

government	and Technology	Accessibility Policy, 2012	hosted at the National Data Centre of the National Informatics Centre

Source: Smriti Parsheera, What's Shaping India's Policy on Cross-Border Data Flows?, Carnegie Endowment for International Peace (2022)

A few general observations emerge from the table. To begin with, there are clear variations in the types of restrictions that have been imposed across and even within related sectors. For instance, while payments-related data has to be stored only in India (subject to limited exceptions), the records of insurance policyholders can be sent abroad so long as the original record is kept in India. This may be the case because the restrictions have been introduced by a range of different actors, across ministries and statutory regulators, which may have differing priorities and approaches.

Further, the nature of instruments utilized to bring about the restrictions also varies widely. Barring the Public Records Act, 1993, which restricts the transfer of public data outside the country, all of the other restrictions emerge either from subordinate legislation like rules, regulations and directives or from other sources like telecommunication licenses, foreign investment policies, advisories and procurement contracts. Finally, as observed elsewhere, many of these requirements came about through processes that were found to be lacking in terms of transparency and deliberative policymaking.[74]

3.2. International arrangements

India has established inter-governmental channels for information sharing through partnerships with several countries. It is a member of INTERPOL, which enables sharing of police information globally and has entered into bilateral mutual legal assistance treaties for cooperation and assistance in criminal matters, including through data exchange provisions, with 42 countries.[75] Further, mechanisms like the Quad alliance and the recent joint statement between India and the US point to arrangements for information sharing on cyber threats and vulnerabilities issues.[76] India also hosts the Information Fusion Centre – Indian Ocean Region, an alliance with 25 partners for information sharing on maritime safety issues.[77]

The EU-India Trade and Technology Council was announced in 2022 to facilitate bilateral cooperation, trade and investment between the two regions. The working group on 'strategic technologies, digital governance and digital connectivity' launched under this initiative is working towards increasing

[74] Rishab Bailey and Smriti Parsheera, Data localisation in India: Paradigms and processes, CSI Transactions on ICT 9, 137–150 (2021) <https://doi.org/10.1007/s40012-021-00337-4>.
[75] Ministry of Home Affairs, Guidelines on Mutual Legal Assistance in Criminal Matters (4 December 2019) <https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines16032020.pdf>.
[76] The White House, Joint Statement from the United States and India (22 June 2023) <https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/22/joint-statement-from-the-united-states-and-india/>.
[77] Information Fusion Centre – Indian Ocean Region <https://www.indiannavy.nic.in/ifc-ior/>.

interoperability between India's and the EU's digital public infrastructure.[78] In 2022, India and the EU also signed a joint declaration on privacy and the protection of personal data along with other partners from the Indo-Pacific region, including Australia, the Republic of Korea, Singapore, and Sri Lanka.[79] The statement speaks of international cooperation on privacy and data protection. It also refers to the importance of data free flow with trust and building 'safeguards for international transfers to enable cross-border data flows by ensuring that the protection travels with the data'.[80]

As a member of G20, India has endorsed the concept of 'data free flow with trust' in ministerial declarations made by the group. The New Delhi declaration made at the 2023 G20 meeting saw a significant emphasis on the role of digital public infrastructure for advancing growth and development. In this context, the G20 members highlighted the role of 'data free flow with trust and cross-border data flows while respecting applicable legal frameworks'.[81] The members also reaffirmed the role of 'data for development', which was another priority area identified by India for its G20 presidency. This refers to initiatives aimed at boosting the production and use of data, particularly in developing countries, to accelerate and measure the progress toward sustainable development.[82]

India has, however, resisted becoming a part of the G20's Osaka Track discussions launched in 2019 to facilitate an international arrangement on cross-border flows to foster innovation and economic growth. This is based on India's position that international rule making on data flows is a trade-related matter and should be a subject of multilateral consensus at the level of the World Trade Organization (WTO).[83] Further, India has also maintained that data constitutes 'a part of national wealth' and developing countries should have an equal say in furthering the use of data for trade and development.[84] For similar reasons, India is not among the 90 countries that are participating in the WTO Joint Initiative on E-commerce,[85] which is not a part of the WTO's formal multilateral negotiations process – it is an alternative plurilateral track being pursued among a subset of the WTO members.

---

[78] Angelos Delivorias, EU-India Trade and Technology Council - At a Glance, European Parliamentary Research Service (January 2024) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757587/EPRS_ATA(2024)757587_EN.pdf>

[79] Joint declaration on privacy and the protection of personal data (23 February 2022) <https://www.eeas.europa.eu/eeas/joint-declaration-privacy-and-protection-personal-data_en>.

[80] Ibid.

[81] G20 New Delhi Leaders' Declaration, India (9-10 September 2023) <https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf> p. 25.

[82] Thierry Soret and Hirofumi Kyunai, The G20 Contribution to the 2030 Agenda in Times of Crises 2019-2023, United Nations Development Programme and the Organisation for Economic Cooperation and Development (2023) <https://www.undp.org/sites/g/files/zskgke326/files/2023-11/undp-oecd-the-g20-contribution-to-the-2030-agenda-in-times-of-crises-2019-2023-v2.pdf> p. 61.

[83] Ministry of External Affairs, "Transcript of Media Briefing by Foreign Secretary After BRICS Leaders' Informal Meeting in Osaka," Indian Ministry of External Affairs (28 June 2019) <https://www.mea.gov.in/media-briefings.htm?dtl/31516/Transcript_of_Media_Briefing_by_Foreign_Secretary_after_BRICS_Leaders_Informal_meeting_in_Osaka>.

[84] Ibid.

[85] WTO Joint Initiative on E-commerce <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#participation>.

Finally, issues of privacy and free flow of data have also come up to a limited extent in the context of India's bilateral and regional trade agreements. The India–Singapore Comprehensive Economic Cooperation Agreement identifies the importance of privacy protections but also cautions against this becoming an 'arbitrary or unjustifiable discrimination against the other Party or its investors' or a disguised restriction on investments or trade.[86] The agreement between India and Japan contains a provision on the transfer and processing of financial information. It restricts the parties from taking 'measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means' where such transfers are necessary for the conduct of the ordinary business of a financial service supplier.[87] However, it is clarified that the parties are not restricted from adopting measures to protect personal data and privacy so long as such right is not used to circumvent the provisions of the agreement.

In 2022, India entered into a comprehensive economic partnership agreement with the UAE. Following a light-touch approach, the agreement provides that the parties 'shall endeavour to promote electronic information flows across borders subject to their laws and regulatory frameworks'.[88] India is now in the process of negotiating a free trade agreement with the UK in which the latter is keen on including more definitive provisions on free cross-border flows and restrictions on data localisation.[89] While the DPD Act has brought some clarity regarding India's position on these issues, it has left the door open for data flow restrictions under other laws suggesting that India may still demand to retain domestic policy space on this issue.

Its cautious approach towards data flow discussions in international agreements is also reflected in the ongoing discussions on the Indo-Pacific Economic Framework for Prosperity. Launched in 2022 as a US-led initiative, this framework seeks to foster 'cooperation, stability, prosperity, development, and peace' among 14 countries in the Indo-Pacific region.90 The framework is structured around four pillars – trade, supply chains, clean economy and fair economy. Of these, India has joined all the pillars except the first one on trade, which includes discussions on cross border data flows. As of now, India has chosen to maintain an observer status in the discussions under this pillar.91 The direction of the discussions under

[86] Articles 6.11(1) and 7(1), Comprehensive Economic Cooperation Agreement between India and Singapore. Also see World Economic Forum, Advancing Data Flow Governance in the Indo-Pacific: Four Country Analyses and Dialogues (April 2021) <https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf> p. 9-10.

[87] Annex 4, Section 6, Comprehensive Economic Cooperation Agreement between India and Japan <https://commerce.gov.in/wp-content/uploads/2021/01/IJCEPA_Basic_Agreement.pdf>.

[88] Article 9.11, Comprehensive Economic Partnership Agreement (CEPA) between India and the United Arab Emirates (2022) <https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf>.

[89] Amiti Sen, India-UK FTA: Efforts on to iron out contentious areas like IPR, digital trade, environment, labour, Hindu Businessline (14 July 2023) <https://www.thehindubusinessline.com/economy/india-uk-fta-efforts-on-to-iron-out-contention-areas-like-ipr-digital-trade-environment-labour/article67080214.ece>.

[90] Office of the United States Trade Representative, Indo-Pacific Economic Framework for Prosperity <https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef>. The participating countries are Australia, Brunei, Fiji, India, Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, Vietnam and the United States of America.

[91] Ministry of Commerce and Industry, Government of India, Indo-Pacific Economic Framework for Prosperity (IPEF) Supply Chain Agreement signed by the 14 IPEF Partners, Press Information Bureau (17 November 2023)

the trade pillar, and indeed India's approach towards it, may, however, change in light of the US Trade Representative's announcement of the reversal in the US's position towards pursuing data free flow provisions in WTO discussions.[92] Similar to India's stated position on this issue, the US now seems to be interested in reserving space for domestic policy making on issues relating to data governance, privacy, competition and online regulation, prioritizing these over the free flow of data.[93]

4. Conclusion

India's evolving position on data protection has been influenced by a range of factors. When the deliberations process began in 2017, India had recently recognized the fundamental right to privacy. The GDPR came into effect around the same time, and it became a logical base for the formulation of India's first draft bill, although there were some notable divergences, as with the issue of data localisation. By the time the DPD Act came to be enacted in 2023, the policy mood had shifted towards a more light touch approach. This is reflected in the leaner scope and structure of the law, which now covers only digital data, has a reduced breadth of rights and obligations, and replaces the idea of a data protection regulator with a board that has a narrower enforcement mandate. This shift was accompanied by a conscious distancing from the idea of borrowing from frameworks like the GDPR and assertions of India's independent standards of data regulation.[94]

The dilution in the restrictions on cross border data flows also speaks to this move toward a leaner regulatory framework. Yet, while the DPD Act adopts a fairly liberal approach towards data transfers – of all transfers being permitted unless restricted – it leaves the field open for the emergence of other sector-specific restrictions. India already has numerous such requirements, in fields like payments, telecommunications, and for public records. It is possible that sectoral localisation mandates will continue to proliferate over time.

The DPD Act does not contain any guidance to inform the rationale or processes to be followed by different agencies while adopting such restrictions or by the government while notifying restricted countries. To mitigate these concerns and prevent further fragmentation in the approach, it is recommended that the basic principles, criteria, and processes governing the formulation of data flow restrictions should be identified in the law. For instance, such proposals should be developed through a consultative process, taking into account the different alternatives of conditional transfers and adopting

<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1977529>.

[92] David Lawder, US drops digital trade demands at WTO to allow room for stronger tech regulation, Reuters (26 October 2023) <https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/>.

[93] Patrick Leblond, After USTR's Move, Global Governance of Digital Trade Is Fraught with Unknowns, Centre for International Governance Innovation (11 December 2023) <https://www.cigionline.org/articles/after-ustrs-move-global-governance-of-digital-trade-is-fraught-with-unknowns/>

[94] Press Information Bureau, Digital Personal Data Protection Act is a world-class legislation: MoS Rajeev Chandrasekhar (13 August 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357> accessed 30 January 2024.

the least intrusive approach for meeting the identified objectives.

While the DPD Act does not specify any preferred mechanisms for data transfers, it clarifies that the appointment of a data processor has to be done pursuant to a valid contract. Accordingly, there seems to be a role for the emergence of model contractual clauses that would govern the relationship between data fiduciaries and processors in line with the requirements of the DPD Act. In the absence of any regulatory mandate for the government or the Board to frame or approve such contracts, stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses following an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.

Finally, it is important to consider how the exemptions available to state agencies for surveillance, law enforcement and other designated purposes might interact with the discussions on data flows. The DPD Act does little in terms of reforming the process for interception of communications and data access by law enforcement agencies. These aspects continue to be governed under other laws like the Information Technology Act, 2000 and the Telecommunications Act 2023, which do not have safeguards like judicial approval of information request, notice to the individual, transparency requirements, and redress mechanisms.[95] India also does not have other standalone laws to govern its surveillance and intelligence agencies. In 2011, an attempt towards bringing about such a regulatory framework was made through a private member bill drafted by a Parliamentarian, Manish Tewari.[96] The bill lapsed in 2012 and was reintroduced in the Parliament in 2019 as the Intelligence Services (Powers and Regulation) Bill, 2019 but has not seen any action since then.[97]

Further, the exceptions created under the DPD Act, particularly under Section 17(2), allow for the complete exclusion of agencies from the scope of the data protection law on grounds like sovereignty and integrity of India, security of the State, and public order. The provision also goes on to exclude any further processing by the government of the data that is furnished to it by an exempted agency. This provision may at some point be subjected to a constitutional challenge to test its validity against the fundamental right to privacy, as is already being done in a bunch of pending petitions challenging the country's existing surveillance regime before the Supreme Court.[98]

Besides being violative of citizens' privacy rights, unchecked powers of law enforcement and intelligence agencies are also detrimental to the free flows of data into the country. For instance, soon after the enactment of the DPD Act, a question came up in the European Parliament about the "interference of

[95] Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, Use of Personal Data by Intelligence and Law Enforcement Agencies, National Institute of Public Finance and Policy (1 August 2018) <https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data>.

[96] Manish Tewari, Intelligence Agencies Need Greater Scrutiny, Congress Sandesh (12 July 2021) <https://inc.in/congress-sandesh/comment/intelligence-agencies-need-greater-scrutiny>.

[97] Intelligence Services (Powers and Regulation) Bill, 2019 <https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/249%20of%202019%20as.pdf?source=legislation>

[98] The Wire, Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State (14 January 2019) <https://thewire.in/law/supreme-court-pil-centre-snooping>.

Indian intelligence services through digital surveillance and the Indian Parliament's apparent lack of control over the intelligence services' actions" and its impact on GDPR adequacy.[99] The response indicated that the European Commission was not engaged in any adequacy talks with India at that point.[100]

As shown by the Schrems II decision, the domestic surveillance and government data access regime is also relevant for other transfer mechanisms besides adequacy. Independently, the situation described above may also interfere with India's plans of boosting its data centre infrastructure and inviting the setting up of data embassies – currently, there is no clarity on how the scope of surveillance powers might interact with the potential creation of such embassies. All of these factors point to the necessity of bringing legislative reforms to strengthen the surveillance and law enforcement framework in India.

To summarize, the paper makes three recommendations on issues related to cross border data flows:

- First, it recommends that, in order to minimize fragmentation and uncertainty, the law should set out the basic principles, criteria, and processes to govern the adoption of any sectoral data flow restrictions. The government's power to impose restrictions on data flows to specific countries should also be bound by such reasonable and identified criteria.
- Second, it suggests that stakeholders from the industry can voluntarily take up the initiative of developing model/ standard clauses that would meet the requirements of the DPD Act, and ideally go beyond that, through an open and consultative process. This can serve as a mechanism for building trust among data fiduciaries and processors and facilitating the ease of regulatory compliance.
- And third, the paper makes a case for legislative reforms to strengthen the country's surveillance and law enforcement framework. Besides being violative of citizens' privacy rights, unchecked powers of law enforcement and intelligence agencies are also detrimental to the flow of data into the country.

[99] Markéta Gregorová, Adequacy of India's data privacy law with regard to EU GDPR standards, Parliamentary question - P-002961/2023 (6 October 2023) <https://www.europarl.europa.eu/doceo/document/P-9-2023-002961_EN.html>.

[100] Answer given by Mr Reynders on behalf of the European Commission, Parliamentary question - P-002961/2023(ASW) (6 December 2023) <https://www.europarl.europa.eu/doceo/document/P-9-2023-002961-ASW_EN.html>.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

COUNTRY DEEP DIVE 3: CHINA

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

Foreword

China's digital economy has thrived over the past decade, making China a full global player with significant trade partnerships. China has set forth a horizontal data governance framework consisting of three main pillars: the Cybersecurity Law (CSL), Data Security Law (DSL), and the Personal Information Protection Law (PIPL) enacted in 2021. The PIPL acts as a foundational layer and applies to both private and public entities, although it is supplemented by other laws and regulations. Most notably, public entities are governed by the PIPL, while being subject to additional requirements stemming from law enforcement and surveillance laws. Overall, the data governance framework aims to strike a balance between two competing interests: the "safe flow" and "free flow" of data. The PIPL applies to electronic information related to identifiable individuals, which is broadly defined, and extends its subject-matter extraterritorially. The PIPL comprises key data protection principles such as lawfulness, fairness, necessity, sincerity, and purpose limitation. While drawing inspiration from the European Union's regulatory framework, it also bears distinct Chinese characteristics, notably a bespoke hierarchy of transfer tools and stringent restrictions set on "critical information infrastructure operators (CIIOs)" and "important data".

Chinese data protection framework has drawn significant criticism due to its shortcomings in upholding constitutional rights, the extensive surveillance powers wielded by public authorities, the proliferation of administrative departments with seemingly overlapping jurisdictions, and their insufficient independence. Despite PIPL being in force for two years, the absence of detailed guidelines on regulated cross-border data transfer tools has created legal uncertainty. Industry stakeholders have called for more clarity amidst evolving guidelines. Rooted in the concept of digital sovereignty, China's approach to data governance seeks not only to safeguard citizen rights but also to strengthen cybersecurity and national security. On the global stage, China has been actively championing its vision, and indirectly challenging other jurisdictions to reassess their positions. Nonetheless, translating China's domestic regulatory objectives into international standards remains a complicated task.

1. Context

China is the second most populous country worldwide.[1] As of June 2023, the number of internet users in China had reached 1.079 billion, showing an increase of 11.09 million people compared with December 2022, with an internet penetration rate of 76.4%.[2] This makes China the largest digital population in the world.[3]

As one of the world's three most prominent trading partners, alongside the European Union and the USA, China plays a significant role in international trade, investment, and economic cooperation.[4] The People's

[1] Data based on the July 2023-July 2024 estimates from the United Nations Population Division. https://www.worldometers.info/world-population/population-by-country/
[2] https://news.cctv.com/2023/08/28/ARTIjd0yIrXKjLS5XCsef0x1230828.shtml
[3] https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
[4] European Commission, 'EU Trade Relations with China' (*European Commission*, 9 August 2023)

Republic of China (PRC) has bilateral investment agreements with over 100 countries and economic unions, including Austria, the Belgium-Luxembourg Economic Union, Canada, France, Germany, Italy, Japan, South Korea, Spain, Thailand, and the United Kingdom. China's Free Trade Agreement (FTA) partners include ASEAN, Singapore, Pakistan, New Zealand, Chile, Peru, Costa Rica, Iceland, Switzerland, Maldives, Mauritius, Georgia, South Korea, Australia, Cambodia, Hong Kong, and Macao.[5]

In recent years, China has become one of the countries that stand out in terms of its capacity to engage in and benefit from the data-driven economy.[6] With the rapid development of internet and communication technologies, China's technological influence is being felt globally.[7] This trend has resulted in the global reach of Chinese technologies, and the fostering of data exchanges between China and numerous countries, including the BRICS countries (Brazil, Russia, India, and South Africa), and Singapore.[8] Products and services offered by Chinese companies such as Huawei, Alibaba and TikTok have increased their market shares in many countries.[9]

With the rise of the digital economy and digital trade, China's data protection regime has been significantly transformed in recent years. The introduction of a comprehensive piece of data protection legislation, the Personal Information Protection Law (PIPL), modelled after the EU's GDPR,[10] represents a noteworthy advancement. However, the Chinese data protection framework is still in the making and continues to raise serious challenges, particularly when compared with standards adopted by key trade partners, such as the EU.[11]

2. China's Data Protection and Cybersecurity Model

<https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en> accessed 25 August 2023.

[5] China - Trade Agreements' <https://www.trade.gov/country-commercial-guides/china-trade-agreements> accessed 2 January 2024.

[6] UNCTAD, 'Cross-Border Data Flows and Development: For Whom the Data Flow' (2021) <https://unctad.org/system/files/official-document/der2021_en.pdf> accessed 9 August 2022.

[7] Munich Security Conference, 'Munich Security Report 2020' (2020) <https://securityconference.org/en/publications/munich-security-report-2020/> accessed 10 August 2020.

[8] Ministry of Science and Technology of the People's Republic of China, 'China Participates in the First Meeting of the Steering Committee of BRICS Technology Transfer Center Network' <https://en.most.gov.cn/pressroom/202206/t20220622_181227.htm> accessed 19 February 2024.

[9] 'Kristin Shi-Kupfer: "China Sees Digitalization as a Chance to Increase Its Global Footprint"' (*Merics*, 8 April 2019) <https://merics.org/en/podcast/kristin-shi-kupfer-china-sees-digitalization-chance-increase-its-global-footprint> accessed 31 May 2023.

[10] Xinbao Zhang (张新宝), *Personal Information Protection Law of the People's Republic of China - A Commentary (中华人民共和国个人信息保护法释义)* (People's Publishing House (人民出版社) 2021).

[11] Yueming Zhang, 'Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-Border Transfers from the EU to China' (2023) 14 European Journal of Law and Technology.

2.1. Constitutional protection

First of all, it is relevant to unpack the connection between the protection of human rights, including the rights to privacy and data protection, and China's constitutional framework. China's current Constitutional Law was adopted on 4 December 1982 and amended in 1988, 1993, 1999, 2004, and 2018. Article 33 of the Chinese Constitution, introduced by the 2004 amendment, states that "the state respects and protects human rights".[12] The Constitution of China also protects "personal dignity", as specified in Article 38: "*the personal dignity of citizens of the People's Republic of China shall not be violated*". Furthermore, Article 35 of the Constitution refers to freedom of expression and states that the "*citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession, and of demonstration*." The Constitution protects the right to freedom of the correspondence [13] and privacy of the correspondence[14] but does not include a general and widely encompassing right to privacy. No express constitutional protection of data protection rights exists, either.

In academic debate, Chinese scholars have proposed a reconstruction of the concept of "human rights" taking into account the development of digitalisation and related changes in society.[15] Scholars have proposed that the constitutional protection of human rights provides a ground to recognise "the right of personal information self-determination"[16] as well as the right to protection of personal information.[17] Yao argues that the right to the protection of personal information can be recognised as a "fundamental human right" in light of Article 33 of the Constitution.[18] Wang considers that "personal dignity", as protected by Article 38 of the Constitution, may provide a ground for protecting personal information.[19] Peng suggests that the right to the protection of personal information should be recognised as a new "basic constitutional right" in order to help form a more detailed personal information protection framework.[20]

---

[12] Article 33 of China's Constitution. Peilin Yu (于沛霖), 'Analysis on the Legal Relationship about 'State Respects and Protects Human Rights ("国家尊重和保障人权"之法律关系解读)' (2007) 06 Journal of Law (法学杂志) 28.

[13] Article 40 of China's Constitution.

[14] Article 39 of China's Constitution.

[15] Changshan Ma (马长山), '"Fourth Generation Human Rights" and Their Protection in the Context of a Smart Society (智慧社会背景下的"第四代人权"及其保障)' (2019) 05 China Legal Science (中国法学) 5.

[16] Hong Zhao (赵宏), 'The Protection Status and Legislative Trend of Information Self-determination Right in China (信息自决权在我国的保护现状及其立法趋势前瞻)' (2017) 01 China Law Review (中国法律评论) 147.

[17] Xixin Wang (王锡锌) and Chun Peng (彭錞), 'The Constitutional Basis of the Personal Information Protection Legal System (个人信息保护法律体系的宪法基础)' (2021) 15 Tsinghua Law Review (清华法学) 6.

[18] Yuerong Yao(姚岳绒), 'The Proof of Information Self-Determination as a Fundamental Right in China （论信息自决权作为一项基本权利在我国的证成）' (2012) 04 Political Science and Law (政治与法律) 73.

[19] Kai Wang (王锴), 'The General Personality Rights in the Constitution and Their Impact on Civil Law (论宪法上的一般人格权及其对民法的影响)' (2017) 03 China Legal Science (中国法学) 115.

[20] Chun Peng (彭錞), 'Personal Information Protection from the Perspective of the Constitution: Clarification of

However, the judiciary has not acknowledged this debate. Nor has it influenced lawmakers. As a civil law country, China cannot through case law create the constitutional right to privacy and data protection without an explicit ground (as it is possible in common law countries, such as the US).[21] Furthermore and most significantly, as there is no constitutional court in China, the Constitution is generally regarded as "non-justiciable".[22] This implies that Chinese courts are not empowered to invalidate a law or a regulation on the ground that it violates the Constitution.[23]

2.2. Relevant general rules

The general data protection and privacy framework in China encompasses several legislative sources, including the Civil Code, the Criminal Law, and the Consumer Protection Code.

It is worth noting that the right to data protection is protected as a civil right. On 28 May 2020, China adopted the Civil Code, which came into force on 1 January 2021. The Civil Code replaced several legislative acts, namely the General Rules of the Civil Law (2016), the Contract Law (1999), the Property Law (2007), the Tort Liability Law (2009), etc.[24] The Civil Code is the first Chinese law to carry the title of "code" and aims to strengthen the protection of people's rights. The Civil Law of China protects natural persons' right to privacy[25] and personal information.[26] Specifically, Article 1032 of the Civil Code states that "a natural person enjoys the right to privacy. No organization or individual may infringe upon the other's right to privacy by prying into, intruding upon, disclosing, or publicizing others' private matters". Article 1034 of the Civil Code states that "personal information is the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person". Under the section on the "right to personality", the Civil Code includes six articles on the right to personal information. The Civil Code includes a definition of "personal information".[27] The Civil Code also specifies the basic data processing principles of lawfulness, justification, and necessity,[28] the circumstances for

---

Nature, Strength Setting and Mechanism Coordination (宪法视角下的个人信息保护：性质厘清、强度设定与机制协调)' (2022) 04 Law and Modernization (**法治**现代化研究).

[21] Yang Feng, 'The Future of China's Personal Data Protection Law: Challenges and Prospects' (2019) 27 Asia Pacific Law Review 62.

[22] Graham Greenleaf, 'China—From Warring States to Convergence?', *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press 2014).

[23] Paul De Hert and Vagelis Papakonstantinou, 'The Data Protection Regime in China' (European Parliament, Directorate-General for Internal Policies 2015) PE 536.472.

[24] Civil Code of the People's Republic of China (《**中**华人民共和国民法典》), adopted by National People's Congress on 28 May 2020, enforced on 1 January 2021. (Hereinafter referred to as "Civil Code" or "Civil Code of China")

[25] Article 1032 of the Civil Code.

[26] Article 1034 of the Civil Code.

[27] Article 1034 of the Civil Code.

[28] Article 1034 of the Civil Code.

exemption from civil liability for processing personal information,[29] the right to consult, copy, rectify and delete personal information,[30] data security principles and obligations[31] as well as the confidentiality of personal information.[32]

In 2013, the National People's Council Standing Committee amended China's Consumer Protection Law to include provisions for the protection of personal information.[33] The Consumer Protection Law provides rules governing the collection and processing of personal information by "online retailers", and sets forth the general data protection principles of legality, rationality, and necessity.[34] The principles included in the Consumer Protection Law are largely identical to the earlier 2012 SC-NPC Decision.[35] These provisions apply to all industries, including companies that provide goods and services within China, in both online and offline contexts, and thus extend the data protection principles to more sectors.[36] The Consumer Protection Law also provides for civil liabilities and administrative enforcement in case of infringement of the obligations to protect personal information.[37] However, data subject rights of access, rectification, and deletion of personal information are missing from this set of rules.[38]

Additionally, according to Article 253(1) of China's Criminal Law, the crime of infringing on citizens' personal information involves that selling or providing a citizen's personal information in violation of state regulations may result in a maximum three-year imprisonment or criminal detention, along with a fine for serious cases, or a fine along with imprisonment ranging from three to seven years for especially serious cases.

2.3. Three main pillars of data protection and cybersecurity in China

With the rise of the digital economy and digital trade, China's data protection regime has undergone significant transformations. Overall, the three main pillars of China's data governance framework are the

[29] Article 1046 of the Civil Code.
[30] Article 1037 of the Civil Code.
[31] Article 1038 of the Civil Code.
[32] Article 1039 of the Civil Code.
[33] Law of the People's Republic of China on the Protection of Consumer Rights and Interests (2013 Amendment) (《中华人民共和国消费者保护法》), amended by the National People's Congress Standing Committee on 25 October 2013, enforced on 15 March 2014.
[34] Article 29(1) Consumer Protection Law.
[35] The 2012 National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection ("2012 NPC-SC Decision") marked the inception of China's data protection regulations. See, Greenleaf, 'China—From Warring States to Convergence?' (n 20).
[36] Graham Greenleaf and George Tian, 'Data Protection Widened by China's Consumer Law Changes' (2013) 126 Privacy Laws & Business International Report 27.
[37] Article 50 Consumer Protection Law.
[38] See, Greenleaf and Tian (n 36).

Personal Information Protection Law (PIPL),[39] the Cybersecurity Law (CSL),[40] and the Data Security Law (DSL).[41] Notably, the general rules mentioned in the previous section have not been abrogated by the PIPL.

Despite the introduction of several provisions in China's Consumer Protection Law, China did not have a comprehensive data protection framework until 2021. This changed on 20 August 2021, when China passed its first comprehensive data protection law, which came into force on 1 November 2021. The PIPL is modelled, at least in part, on foreign data protection regimes, most notably the GDPR.[42] The PIPL was developed with the aim of "protecting interests of personal information, regulating personal information processing activities, and promoting the reasonable use of personal information".[43] The PIPL is also the first data protection law in China that applies to public authorities.[44]

In addition to the PIPL, China's data governance framework also comprises security laws: the CSL and the DSL. The CSL, which came into force on 1 June 2017, included some of the most comprehensive data protection principles at that time. Overall, the CSL focuses on national data security and includes requirements related to data localisation, critical infrastructure protection, and cyber incident response.[45] The DSL, which was adopted on 10 June 2021, aims to ensure the security of data with a view to protect national security and public security interests. The DSL covers both personal and non-personal data.[46]

Notably, Chinese laws, like the CSL, the DSL and the PIPL, often only contain general principles and require more detailed implementation and interpretation rules to make them enforceable to be issued by data protection departments such as the CAC.[47] As a result, in recent years, there has been an abundance of implementing regulations and guidelines in China to fill the interpretative gaps left by these three laws.[48]

The EU's influence on the Chinese data governance framework, particularly the PIPL, is manifest.[49]

---

[39] The Personal Information Protection Law of the People's Republic of China (《中华人民共和国个人信息保护法》), adopted by SC-NPC on 20 August 2021, enforced on 1 November 2021.

[40] The Cybersecurity Law of the People's Republic of China (《中华人民共和国网络安全法》), adopted by SC-NPC on7 November 2016, enforced on 1 June 2017.

[41] The Data Security Law of the People's Republic of China (《中华人民共和国数据安全法》), adopted by SC-NPC on 10 June 2021, enforced on 1 September 2021.

[42] Guan Zheng, 'Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China' (2021) 43 Computer Law & Security Review 105610.

[43] Article 1 of the PIPL.

[44] Article 33 of the PIPL.

[45] Graham Greenleaf and Scott Livingston, 'China's New Cybersecurity Law – Also a Data Privacy Law?' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2958658 <https://papers.ssrn.com/abstract=2958658> accessed 29 January 2020.

[46] Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 Journal of Cybersecurity tyac011.

[47] European Data Protection Board, 'Legal Study on Government Access to Data in Third Countries' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en> accessed 10 January 2022.

[48] 'Law in China - DLA Piper Global Data Protection Laws of the World' <https://www.dlapiperdataprotection.com/index.html?t=law&c=CN> accessed 13 December 2023.

[49] Daniel Solove, 'China's PIPL vs. the GDPR: A Comparison' (2021) <https://teachprivacy.com/chinas-pipl-vs-gdpr-a-

However, regarding cross-border data transfer rules, lawmakers in China have been developing an original regime with several Chinese characteristics.[50] Overall, the Chinese data transfer regime aims to strike a balance between different competing objectives: the growth of the digital economy, the protection of personal data, and the protection of national security and cyber sovereignty interests.

2.4. Core Personal Data Protection Rules

2.4.1. Personal data under the PIPL

The PIPL defines personal information as "all kinds of information recorded by electronic or other means *related to identified or identifiable natural persons*".[51] This appears similar to the definition given in Article 4(1) of the GDPR.

In addition, information that has been anonymised is excluded from the material scope of the PIPL.[52] Anonymisation in the PIPL refers to the process of processing personal information "to make it impossible to identify specific natural persons" and "impossible to restore".[53] The definition of anonymisation thus uses absolutist language, which will be difficult to interpret on the ground given the practical impossibility of eliminating all re-identification risks, even with the most sophisticated techniques. Yet, anonymisation is of particular relevance in the context of cross-border data transfers, as it offers, at least in principle, a means to avoid (some) restrictions. The anonymisation standard ultimately adopted by China should therefore be carefully considered to fully grasp the implications of the cross-border data transfer restrictions.

2.4.2. Scope of the PIPL

The PIPL applies to the "processing" of personal information. Article 72 of the PIPL excludes the application of the law under a few circumstances. Purely personal or household activities are exempted from the application of the PIPL. This seems to be in line with the GDPR.[54] Moreover, the PIPL indicates that the specific laws that govern the "personal information processing of statistical or archives administration activities organised and implemented by the governments" will prevail in case of conflict.[55]

Under Article 3 of the PIPL, the law applies to the activities of processing personal information both *within the borders* of the PRC and *outside the borders* of the PRC under three circumstances.[56] These circumstances include:

---

comparison> accessed 12 December 2023.

[50] Graham Greenleaf, 'China Issues a Comprehensive Draft Data Privacy Law' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3795001 <https://papers.ssrn.com/abstract=3795001> accessed 23 March 2022.

[51] Article 4 PIPL.

[52] Article 4 PIPL.

[53] Article 73(4) PIPL.

[54] Article 2 GDPR.

[55] Article 72 (2) PIPL.

[56] Article 3 PIPL.

1. Where the purpose is to provide products or services to natural persons inside the borders,

2. When conducting analysis or assessment of activities of natural persons inside the borders,

3. Other circumstances provided in laws or administrative regulations.

The territorial scope of the PIPL, as determined by Article 3, confirms the legislator's intention to protect personal information of both Chinese residents and foreign people located in China.

With regard to the territorial scope set by Article 3(1), the PIPL applies to the "processing activities" carried out within the territory of China, while an "establishment" in China is not required. As a result, a foreign company with no establishment in China can still be regulated by the PIPL if the processing activities are carried out in China. By contrast, even if a covered entity is established in China, it does not necessarily fall within the scope of Article 3(1) if all its data processing activities are only carried out overseas.[57]

2.4.3. Data processing principles

The PIPL sets forth a number of fundamental personal information protection principles. These principles comprise lawfulness, fairness, necessity, and sincerity,[58] purpose limitation and data minimisation,[59] transparency,[60] data quality,[61] accountability and data security. [62]

2.4.4. Data subjects' rights

Similar to the EU GDPR, the Chinese data protection legal framework grants individuals a series of data protection rights.

The PIPL enhanced the protection of individuals' data protection rights that already existed in the Chinese Civil Code and recognised a series of other rights. It provides that an individual has: the right to know and decide,[63] the right to access,[64] the right to rectification,[65] the right to delete,[66] and the right to request an explanation.[67]

The PIPL does not provide a right to object to processing in general, although the right to decide found in Article 44 of the PIPL could be interpreted as covering this prerogative. Further, the PIPL also aims to protect individuals against automated decision-making and profiling. It recognises an individual's right to

---

[57] See Samuel Yang, 'A Look at the Extraterritorial Applicability of China's Newly Issued PIPL: A Comparison to the EU's GDPR' <https://iapp.org/news/a/a-look-at-the-extraterritorial-applicability-of-chinas-newly-issued-pipl-a-comparison-to-the-gdpr/> accessed 15 January 2023.
[58] Article 5 PIPL.
[59] Article 6 PIPL.
[60] Article 7 PIPL.
[61] Article 8 PIPL.
[62] Article 9 PIPL.
[63] Article 44 PIPL.
[64] Article 45 PIPL.
[65] Article 46 PIPL.
[66] Article 47 PIPL.
[67] Article 48 PIPL.

refuse decisions made solely through automated decision-making when the automated decision-making produces decisions that may have "a major influence on the rights and interests of the individual". Those conducting automated decision-making for commercial purposes must simultaneously provide the option to not target an individual's characteristics or provide the individual with a convenient method to refuse.

2.4.5. Lawful grounds for data processing

The lawfulness of personal information processing means that the processing should be grounded on a valid legal basis. Both the GDPR and PIPL include an exhaustive list of legal bases to legitimise the processing of personal information, but these two lists are not identical. Under the PIPL, processing of personal information must be based on one of six lawful grounds, with an exception if "other circumstances are provided in laws and administrative regulations".[68]

These grounds are:

- consent,
- necessary to conclude or fulfil a contract with the individual,
- necessary to fulfil statutory responsibilities or statutory obligations,
- necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions,
- reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, and
- processing of the personal information disclosed by the individuals or other legally disclosed personal information.[69]

With respect to consent, the PIPL further imposes certain substantive and procedural requirements in Articles 14 and 16. Consent for processing of personal information must be obtained 1) under the precondition of full knowledge, 2) with a voluntary and explicit statement of wishes[70] and 3) on the basis that it is revocable.[71] The PIPL also indicates several circumstances under which specific consent is required, which include the use of facial recognition,[72] transferring personal information beyond the borders,[73] and processing sensitive personal information. Notably, the PIPL drafters have chosen to adopt a broad and open definition of sensitive personal information.[74] Children in China cannot give consent

[68] Article 13(7) PIPL.
[69] Article 13 PIPL.
[70] Article 14 PIPL.
[71] Article 16 PIPL.
[72] Article 27 PIPL.
[73] Article 39 PIPL.
[74] Article 30 PIPL. Under the PIPL sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of

until they are 14 years old. For children younger than 14, parental consent is needed.[75]

The second lawful basis is contractual necessity. The PIPL allows processing of personal information when "necessary to conclude or fulfil a contract in which the individual is an interested party".[76] In order to achieve this, the scope of the personal information processed must be limited to the scope of the contract. Scholars have been calling for a restrictive interpretation of the "contractual necessity" test.[77]

The third lawful basis is the necessity to fulfil statutory duties and responsibilities or statutory obligations.[78]

The fourth lawful basis, i.e., responding to "sudden public health incidents or protect natural persons' lives and health," finds some of its roots in the COVID-19 pandemic. Under such emergency conditions where it is impossible to notify individuals in a timely manner, it is required to notify them after the conclusion of the emergency circumstances.[79]

The fifth lawful basis allows "within a reasonable scope to implement news reporting, public opinion supervision for the public interest".[80] "Public opinion supervision" generally refers to critical reporting by news organisations or social media users regarding public affairs or public authorities' activities.[81] The reference to the "public interest" should imply that news reporting and public opinion supervision aim to fight against "immoral, illegal and criminal matters or to supervise public power and to uphold social justice".[82]

The sixth lawful basis covers "personal information disclosed by the individuals or other legally disclosed personal information".

Of note, comparing the PIPL's list to the GDPR's list, one important difference is the absence of the legitimate interest ground within the PIPL's list. This may mean that both the consent and the contractual necessity legal bases will have to be interpreted broadly to the detriment of the principle of purpose limitation.

---

14. See Article 28 PIPL.

[75] Article 15 PIPL.

[76] Article 14 (2) PIPL.

[77] Weixing Shen (申卫星) and Xu Yang (杨旭), 'On the Restrictive Application of the Conclusion of a Contract as the Legal Basis for Personal Information Processing (论订立合同作为个人信息处理合法性基础的限缩适用)' (2022) 04 Nanjing Journal of Social Science (南京社会科学) 76.

[78] Article 14 (3) PIPL.

[79] Article 19 PIPL.

[80] Article 999 of the Civil Code.

[81] Xiao Cheng (程啸), The Interpretation of Personal Information Protection Law of the People's Republic of China (个人信息保护法理解与适用) (China Legal Publishing House (中国法制出版社有限公司) 2021).

[82] Cheng (程啸) (n 81).

2.4.6. *Data protection enforcement*

The effectiveness of data protection rules depends on robust enforcement mechanisms. China does not have one independent supervisory authority in charge of the enforcement of data protection rules. Instead, enforcement prerogatives are shared among several administrative units. The PIPL identifies the relevant departments that are responsible for fulfilling personal information protection duties, which include:[83]

Departments	Comments
State cybersecurity and informatisation department[84]	Responsible for comprehensive planning and coordination of personal information protection enforcement and related supervision and management work
Relevant State Council departments[85]	Responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities
County-level and higher People's Governments' relevant departments	Such departments' responsibilities are determined according to relevant State regulations

Table 1 Relevant departments that are responsible for fulfilling the personal information protection duties in China

Overall, these departments are not independent authorities, but departments affiliated to the State Council or other executive administrations. The PIPL includes an overview of the tasks and powers of such departments fulfilling the personal information protection duties, which are: [86]

[83] Article 60 PIPL.
[84] Namely, the Cyberspace Administration of China (CAC).
[85] For instance, the Ministry of Industry and Information Technology (MIIT).
[86] Article 61 PIPL.

1. Conducting personal information protection education, and guiding and supervising personal information handlers' conduct of personal information protection work,

2. Accepting and handling personal information protection-related complaints and reports,

3. Investigating and handling unlawful personal information handling activities,

4. Other duties and responsibilities provided in laws or administrative regulations.

The absence of an independent data protection authority has been criticised by Western scholars.[87] The decentralised enforcement model has also been criticised within China. Scholars have found this approach in practice to entail "unclear delineation of responsibilities, individualistic approaches, and deferral of law enforcement actions".[88] It has also been pointed, however, that the creation of a new oversight department may face challenges in terms of human resources, experience and professionalism.[89] During the drafting period of the PIPL, the creation of a separate data protection authority, or a separate body with national responsibility for enforcement of data protection rules, was proposed.[90] However, this approach was not adopted by the PIPL.

On 16 March 2023, the Chinese Communist Party (CCP) Central Committee and the State Council released the plan to establish a new state-level regulatory body, namely the "National Data Bureau" (NDB).[91] The NDB will be responsible for "coordinating the integration, sharing, development and utilisation of data sources and coordinating the promotion of China's digital economy". [92] The relevant discussions and reports from the government are still emerging. The plan, however, clarified that the NDB will not replace the existing competent departments to become an independent oversight authority for data protection issues in China. Instead, the NDB will take the main task of promoting China's digital economy. The Cyberspace Administration of China (CAC) and the NDB will be the two wings of China's data governance framework, with the CAC concentrating on data security and the NDB concentrating on the data economy.[93]

Article 66 of the PIPL empowers the "relevant oversight departments" to impose administrative sanctions. The types of sanctions include correction orders, warnings, confiscation of illegal incomes, and suspension

[87] See De Hert and Papakonstantinou (n 23).

[88] Xinbao Zhang (张新宝), Personal Information Protection Law of the People's Republic of China - A Commentary (中华人民共和国个人信息保护法释义) (People's Publishing House (人民出版社) 2021) 463.

[89] Zhang (张新宝) (n 88) 463.

[90] Yehan Huang and Mingli Shi, 'Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law' (*DigiChina*) <https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/> accessed 4 March 2022.

[91] Jia Xu, 'What Does China's Newly Launched National Data Bureau Mean to China and Global Data Governance?' (*Internet Policy Review*, 25 April 2023) <https://policyreview.info/articles/news/chinas-national-data-bureau-and-global-data-governance> accessed 21 May 2023.

[92] 'Establishment of the National Data Bureau in China (组建国家数据局)' (*Xinhuanet*, 7 March 2023) <http://www.xinhuanet.com/politics/2023-03/07/c_1129419141.htm> accessed 21 May 2023.

[93] Xu (n 91).

or termination of services. If the personal information handler refuses to take such corrective actions, the oversight departments have the power to impose high administrative fines. The PIPL follows the GDPR's approach of a tiered system of fines. As a matter of principle, administrative fines can go up to RMB 1,000,000 (about EUR 132,000) and the responsible individuals can be fined up to one tenth of this amount. When the breach is serious, administrative fines can go up to RMB 50 million (about EUR 6,600,000) or 5% of the previous year's annual turnover, whichever is higher.[94] However, the PIPL itself does not clarify the specific factors to take into account to determine the level of fines, nor the specific oversight departments in charge of issuing the fines.

2.5. Data localisation rules

Overall, China does not impose a blanket prohibition on the transfer of data outside its territorial boundaries. However important restrictions are in place, including storage localisation requirements.

In general, Article 37 of the CSL requires critical information infrastructure operators ("CIIOs") to store personal information and important data generated from critical information infrastructures in China. Article 40 of the PIPL also specifies that "Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatisation department shall store personal information collected and produced within the borders of the People's Republic of China domestically." The PIPL nonetheless provides an exemption from this rule, so that "where they need to provide it abroad, they shall pass a security assessment organised by the State cybersecurity and informatization department".[95] The details of the security assessment are discussed later.

Moreover, Article 36 of the PIPL states that personal information "processed by public authorities" shall be stored within the mainland territory of China, with the caveat that when there is an actual need for transferring personal information abroad, a security assessment must be successfully passed.

2.6. Rules applicable to public authorities

An obstacle to China's participation in global discussions on cross-border data regulations is its domestic surveillance and law enforcement rules. One serious concern is that the Chinese national security and criminal law enforcement system is not in line with EU standards.[96]

The PIPL is the first legal instrument restricting public authorities' activities relating to the processing of personal information. It specifically imposes personal information processing requirements on "state

[94] Article 66 PIPL.
[95] Article 40 PIPL.
[96] European Data Protection Board, 'Legal Study on Government Access to Data in Third Countries' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en> accessed 10 January 2022.

organs" and sets forth seven lawful bases for the processing of personal information in this context.[97]

The PIPL specifies that the processing of personal data by public authorities must not exceed the scope necessary to carry out their responsibilities. Moreover, Article 35 of the PIPL specifies that public authorities must inform data subjects of the fact that their personal information is being processed. In addition, Article 36 of the PIPL states that personal information "processed by public authorities" shall be stored within the mainland territory of China, with strict conditions for data exports from China. Overall, the PIPL's data processing requirements also apply to public authorities, while the PIPL also highlights that the principles such as data minimisation and storage localisation shall be strictly respected by public authorities' when they process personal information.

To note, the PIPL provides various redress mechanisms to individuals when there is a breach by a public authority, including both administrative-oriented compensatory mechanisms and possibilities for judicial remedies. In China, individuals have the right to file a complaint, make a report or an accusation in the event of unlawful processing of personal data, or claim compensation for data privacy breaches before the internal oversight department of each state organ.

Other laws such as the Chinese Criminal Procedure Law as well as national security laws (including the National Security Law,[98] National Intelligence Law,[99] Counter-espionage Law,[100] Counter-terrorism Law[101]) are however also applicable to public authorities.

Furthermore, under the Criminal Procedure Law,[102] personal information deemed to be electronic evidence can be collected and used by criminal investigation authorities in China.[103] Under the Counter-terrorism law, organisations and individuals have the obligation to assist and cooperate with relevant counter-terrorism activities,[104] telecommunications business operators and Internet service providers are specifically required to provide assistance for counter-terrorism work.

Overall, given the wide range of personal information that public authorities can collect, the safeguards

---

[97] Article 33 PIPL.

[98] National Security Law of People's Republic of China (《中华人民共和国国家安全法》), adopted by the SC-NPC on 1 July 2015, enforced on 1 July 2015.

[99] The National Intelligence Law of the People's Republic of China (《中华人民共和国国家情报法》), adopted by the SC-NPC on 27 June 2017, amended by the SC-NPC on 27 April 2018.

[100] The Counter-espionage Law of the People's Republic of China (《中华人民共和国反间谍法》), adopted by the SC-NPC on 1 November 2014.

[101] The Counter-terrorism Law of the People's Republic of China (《中华人民共和国反恐怖主义法》), adopted by the SC-NPC on 27 December 2015, amended by the SC-NPC on 27 April 2018.

[102] The Criminal Procedure Law of the People's Republic of China (《中华人民共和国刑事诉讼法》), adopted by the NPC on 1 July 1979, amended by the NPC on 14 March 2012.

[103] Fan Yang and Jiao Feng, 'Rules of Electronic Data in Criminal Cases in China' (2021) 64 International Journal of Law, Crime and Justice 100453.

[104] Article 9 Counter-terrorism Law.

for personal information processing remain high level and limited.[105]

3. China's cross-border data transfer regime

3.1. Scope

The Chinese cross-border data transfer regime has been established by the PIPL and the CSL. These instruments are supplemented by other measures and standards, which further interpret the data export framework and provide detailed implementation rules.

The CSL provides the general rule on data localisation of "critical information infrastructure operators (CIIOs)". Under the CSL, CIIOs in mainland China must store the collected or generated personal information or important data within mainland China. If it is genuinely necessary to provide such information outside the mainland due to business requirements, they must undergo a security assessment following measures jointly formulated by the State cybersecurity and informatisation departments and relevant State Council departments. Any contrary provisions specified by laws or administrative regulations must be followed.[106]

The transfer of personal data outside the borders of the PRC, for business or other purposes, is regulated by Chapter III of the PIPL. These provisions regulate the transfer of personal information by personal information handlers, who may be natural persons or legal entities, including public authorities.

3.2. Data transfer tools

In general, data transfers to countries outside China must satisfy one of the conditions set out in Article 38 of the PIPL:

- passing a security assessment administered by the CAC;
- undertaking a personal information protection certification run by recognised institutions in accordance with relevant regulations of the CAC;
- executing a standard contract for cross-border transfer provided by the CAC; or
- other bases provided in laws or administrative regulations or by the CAC.

Moreover, all cross-border data transfers initiated from China must be "truly needed": in other words, cross-border data transfers must overcome a "necessity test".[107] Unlike the GDPR, there is no scope for

[105] Mei Liu (**刘玫**) and Yunan Chen (陈雨楠), 'From Conflict to Integration: The Construction of Rules for the Protection of Citizens' Personal Information in Criminal Investigations (**从冲突到融入：刑事**侦查中公民个人信息保护的规则建构)' (2021) 05 Research on Rule of Law (**法治研究**) 34.

[106] Article 37 CSL.

[107] Article 38 of the PIPL.

"derogations". Although this is debated, whatever the means chosen to transfer the data, the personal information handler seems to be obliged to obtain the consent of the individual before transferring personal information abroad. In other words, when transferring personal information outside the territory of China, a separate consent appears to be necessity.[108] Making consent a necessary condition in most, if not all data transfer instances, is however likely to dilute this legal basis.

The framework for cross-border data transfers in China is summarised in Table 2:

Transfer of CII information / personal information over set quantities	**Transfer of non-CII personal information under set quantities**
"Necessity" test	
Pass a security assessment	Meet at least one of the following conditions: (1) Pass a security assessment (2) Certification (3) Standard contract
A separate consent	

Table 2. An overview of legal bases for transfer under the PIPL

Importantly, data exporters are *not* always allowed to freely choose among the three data transfer mechanisms, as the PIPL sets strict requirements for CIIOs[109] and when personal information reaches set quantities (cumulatively 100,000 persons' personal information or 10,000 persons' sensitive personal information).[110] For non-CIIO personal information processed in small quantities, personal information handlers can choose among the three cross-border data transfer tools mentioned above.

3.2.1. Security assessment for cross-border data transfers

The first data export mechanism is to pass a "security assessment". On 7 July 2022, the CAC released the Measures for the Security Assessment of Cross-border Data Transfer,[111] which came into effect on 1 September 2022. The Measures provide more details on the implementation of the "security

[108] Weiqiu Long (龙卫球), *Interpretation of the Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法释义)* (China Legal Publishing House (中国法制出版社有限公司) 2021).

[109] The critical information infrastructure operators ('CIIOs') refer to "infrastructure involving the public communication and information services, power, traffic, water, finance, public service, and e-governance as well as other critical information infrastructure that if it is destroyed, loses its ability to function or encounters data leaks, might seriously endanger national security, national welfare and the people's livelihood, or the public interest". See, Article 31 of the CSL.

[110] Measures for the Security Assessment of Cross-border Data Transfer (《数据出境安全评估办法》) 2022 (State Internet Information Office Order No 11 (国家互联网信息办公室令 第11号).

[111] Measures for the Security Assessment of Cross-border Data Transfer (《数据出境安全评估办法》) 2022 (State Internet Information Office Order No 11 (国家互联网信息办公室令 第11号).

assessment".

Under these measures, the security assessment is necessary in the following circumstances:

- When important data[112] is transferred abroad.
- Where critical information infrastructure operators or data handlers handling the personal information of 1,000,000 or more persons provide personal information overseas.
- Where data handlers providing personal information abroad have cumulatively provided 100,000 persons' personal information or 10,000 persons' sensitive personal information abroad since 1st January of the preceding year.
- Other situations where the State Internet Information Department requires reporting on data export security assessments.[113]

The scope of "security assessment" covers both personal information and "important data." "Important data" is defined as "any data which may endanger China's national security, economic operation, social stability, public health or public security, if it is tampered with, destroyed, leaked, or illegally acquired or used".[114]

The security assessment advocates fora risk-based approach.[115] Specifically, the security assessment requires the data exporter to complete a prior self-assessment of its data transfers. The self-assessment must cover 1) the purposes, scope and methods of the data transfers, 2) the quantity, type and sensitivity of the data as well as the risk that may be brought by the transfers to national security, public interest or the rights and interests of other individuals and organisations, 3) the technical measures and compliance capabilities of the data recipients, 4) the channels for individuals to get remedies for their data protection right, and 5) a contract or document with legal force to set data protection obligations for the data recipients.[116] The security assessment must be submitted to the provincial-level Internet Information Department for review by both the provincial and national levels of the CAC departments.[117]

The circumstances under which security assessments are required are broadly defined. As Zhao points out, in the vast majority of cases, the number and scale of commercial data flows between local and foreign entities is so large that it is easy to meet the security assessment triggers. It will leave only a few

[112] The concept of "important data" refers to "any data which may endanger China's national security, economic operation, social stability, public health or public security, if it is tampered with, destroyed, leaked, or illegally acquired or used", see Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.
[113] Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.
[114] Article 19 of the Measures for the Security Assessment of Cross-Border Data Transfer.
[115] Xiaodong Ding (丁晓东), 'The Jurisprudential Reflection and Institutional Reconstruction of Cross-border Data Transfer: With a Comment on Measures of Out bound Data Transfer Security Assessment (数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》)' (2023) 01 Administrative Law Review(行政法学研究) 62.
[116] Article 5 of Measures for the Security Assessment of Cross-border Data Transfer.
[117] Article 4 of Measures for the Security Assessment of Cross-border Data Transfer.

data-transfer scenarios for the other two mechanisms.[118]

In January 2023, China's first security assessment was approved for data transfers between Beijing Friendship Hospital Affiliated with Capital Medical University and the Medical Center of Amsterdam.[119]

3.2.2. China's Standard Contract

The Chinese Standard Contract, together with the Regulations of Standard Contracts for Cross-border Transfer of Personal Information (the Chinese SCCs Regulations),[120] was unveiled by the Chinese National Information Security Standardisation Technical Committee on 24 February 2023. The Regulations came into force on 1 June 2023 with a six-month grace period running until 1 December 2023. The Chinese Standard Contract can only be used for transferring non-CIIO data, "non-important" data and personal data under set quantities.

It has been argued that the mechanism for data transfers based on the Standard Contract shows China's choice of a risk-based approach and observance of the principle of proportionality regarding transfer issues.[121] Compared with the EU Standard Contractual Clauses, the Chinese Standard Contract does not differentiate between scenarios based on the role of the parties.[122] However, both the EU SCCs and the Chinese Standard Contract recognise third-party beneficiary rights: data subjects are third-party beneficiaries under the Standard Contract. The Chinese Model Contract includes the data subject's rights under the PIPL to be protected by the data importer in the recipient country. The specific rights do not mirror the EU SCCs, but the idea of providing data subjects with the rights to enforce their data rights from the data recipients is similar to the EU SCCs. In case of data breaches, the Chinese Standard Contract requires the personal information importer to promptly take remedial actions and mitigate the impact on relevant individuals. Further, they must notify the breaches to the data exporter, the competent Chinese authority as well as the relevant individuals.

The Chinese Standard Contract provides a series of obligations for personal information handlers. For instance, the regulators stipulate that before transferring personal information abroad, a personal information handler must conduct a Personal Information Protection Impact Assessment (PIPIA) in

---

[118] Jingwu Zhao (赵精武), 'On the Systematization of Data Cross-Border Assessment, Contracts and Authentication Rules (论数据出境评估、合同与认证规则的体系化)' (2023) 01 Administrative Law Review(行政法学研究) 1.

[119] Beijing Daily, Beijing Takes the Lead in Realising Secure and Convenient Cross-border Data Flow for the High-quality Development of Digital Economy, 9 January 2024. https://www.gov.cn/lianbo/difang/202401/content_6925023.htm

[120] National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会), 'The Cyberspace Administration of China Announced the "Standard Contract Measures for the Export of Personal Information" (国家互联网信息办公室公布《个人信息出境标准合同办法》)' <https://www.tc260.org.cn/front/postDetail.html?id=20230224182605> accessed 15 May 2023.

[121] Jing Jin (金晶), 'Standard contractual clauses as a regulatory tool for cross-border transfers of personal information (作为个人信息跨境传输监管工具的标准合同条款)' (2022) 44 法学研究 19.

[122] Reed Smith LLP, 'Cross-Border Data Transfer Mechanism in China and Practical Steps to Take' <https://www.reedsmith.com/en/perspectives/2022/10/cross-border-data-transfer-mechanism-in-china-and-practical-steps-to-take> accessed 8 December 2022.

advance.[123] The PIPIA requirements under the Chinese Standard Contract share conceptual similarities with the Data Protection Impact Assessment (DPIA) mandate outlined in the GDPR although they are systematically triggered. The primary objective of a PIPIA is to identify and evaluate risks associated with individuals' personal data, mitigating the likelihood of data breaches, and ensuring adherence to data protection regulations.[124]

The Chinese Standard Contract also requires data exporters to notify individuals that they are third-party beneficiaries and to mention the individual's right to access, copy, amend, and delete. Moreover, individuals have the right to request a copy of the Standard Contract.[125]

3.2.3. China's certification mechanism

On 24 June 2022, the Security Certification Guidelines on Cross-border Transfer of Personal Information,[126] which serve as the guidelines for the "certification mechanism" were adopted. On 18 November 2022, the CAC issued the Implementation Rules for Personal Information Protection Certification,[127] which also apply to the certification of cross-border data transfers and provide more detailed rules on the procedures for certification. The certification mechanism can be employed for "cross-border processing of personal information between multinational companies or subsidiaries or affiliated companies of the same economic or business entity".[128]

Despite the name "certification mechanism", China's version of the certification process shares more similarities with Binding Corporate Rules (BCRs) as governed by the GDPR.[129] More specifically, personal information handers are required to 1) conduct a self-assessment, 2) sign a data transfer contract or a legally binding document with the data recipients, 3) appoint a Data Protection Officer in China, 4) keep records of the personal information processing activities, 5) identify and notify personal information breaches, and 6) fulfil the obligations of protecting individual rights.[130]

The professional certification institution in China is the "China Cybersecurity Review and Technology and

[123] Article 5 of the Standard Contract Measures for the Export of Personal Information.
[124] 'International: Comparing China's Standard Contract to the EU's SCCs' (*DataGuidance*, 20 June 2023) <https://www.dataguidance.com/opinion/international-comparing-chinas-standard-contract-eus> accessed 2 January 2024.
[125] Article 2 of the Standard Contract Measures for the Export of Personal Information.
[126] National Information Security Standardization Technical Committee, 'Security Certification Guidelines on Cross-Border Transfer of Personal Information (网络安全标准实践指南——个人信息跨境处理活动安全认证规范)' <https://www.tc260.org.cn/front/postDetail.html?id=20220624175016> accessed 9 December 2022.
[127] Cyberspace Administration of China, 'Implementation Rules for Personal Information Protection Certification (个人信息保护认证实施规则)' <http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm> accessed 9 December 2022.
[128] Article 2 of the Security Certification Guidelines on Cross-Border Transfer of Personal Information.
[129] Reed Smith LLP, 'Cross-Border Data Transfer Mechanism in China and Practical Steps to Take' <https://www.reedsmith.com/en/perspectives/2022/10/cross-border-data-transfer-mechanism-in-china-and-practical-steps-to-take> accessed 8 December 2022.
[130] Article 5 of the Security Certification Guidelines on Cross-Border Transfer of Personal Information.

Certification Centre (CCRC)".[131] The process for certification includes five stages: certification application, technical verification, on-site audit, certification decision, and post-certification supervision.[132]

3.3. Recent evolution: the Provisions on Regulating and Promoting Cross-Border Data Transfers

Relatively quickly after its adoption, the enforcement of the first version of the data transfer regime appeared too strict and complicated. On 28 September 2023, the CAC thus published a draft regulation called the "Provisions on Regulating and Promoting Cross-Border Data Transfers".[133] If passed, these regulations will ease certain aspects of China's current cross-border data transfer rules, in particular to the benefit of foreign companies and multinationals.[134] This evaluation signals that China may be in the process of rebalancing the compromise initially set between economic growth and national security interests.[135]

According to the draft regulations, the transfer of data falling under categories like international trade, academic cooperation, transnational manufacturing, and marketing, which do not contain personal information or important data, would not need to go through any of the data transfer mechanisms mentioned in section 3.2 of this report. [136]

With regard to "important data," for which there is no definition yet in the law or related guidance, data transfer approval would only be required once competent authorities either explicitly define what categories of data constitute "important data" or if covered entities are directly notified that their data are "important." The intention is thus to reduce the chilling effect of the restrictions set upon important data by enhancing legal certainty.[137]

The draft regulations also attempt to clarify other key points of the data transfer regime. For instance, there would be no restrictions on the transfer of personal data outside China for the purpose of entering into or performing a contract to which the data subject is a party, such as cross-border shopping, cross-border bank transfers, airline and hotel bookings, and visa processing. The transfer of employee data, as

[131] Cyberspace Administration of China (n 127).
[132] Article 4 of Implementation Rules for Personal Information Protection Certification.
[133] Office of the Central Committee for Network Security and Informatisation, 'Notice of the National Internet Information Office on the Public Consultation on Provisions on Regulating and Facilitating Cross-Border Flow of Data (Draft for Opinion (国家互联网信息办公室关于《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见的通知)' (28 September 2023) <http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm> accessed 13 December 2023.
[134] Arendse Huld, 'China Cross-Border Data Transfer - Regulator Moves to Ease Rules' (*China Briefing News*, 3 October 2023) <https://www.china-briefing.com/news/china-cross-border-data-transfer-draft-regulations-ease-requirements/> accessed 14 December 2023.
[135] Martin Chorzempa and Samm Sacks, 'China's New Rules on Data Flows Could Signal a Shift Away from Security toward Growth | PIIE' (3 October 2023) <https://www.piie.com/blogs/realtime-economics/chinas-new-rules-data-flows-could-signal-shift-away-security-toward-growth> accessed 14 December 2023.
[136] Article 1 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.
[137] Article 2 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.

necessitated by the employment contract and in accordance with relevant laws, such as Chinese employment laws, will also be exempt from the data transfer provisions.[138]

Furthermore, under the draft regulations it would be for the covered entities to interpret the "necessity test" -- they would not have to wait for the regulators to issue their interpretation. This change would affect covered entities that process data of less than a million individuals.[139]

It has been recently reported that Shanghai is set to expedite approvals for foreign firms seeking to transfer local data offshore, presenting another significant relaxation of China's stringent restrictions. The initiative, discussed with representatives of foreign firms in the past few weeks, aims to attract foreign investors amidst China's economic challenges, offering a potential solution to delays and concerns caused by the 2022 regulations requiring security reviews for important offshore data transfers.[140]

4. International commitments

China is a member of the Asia-Pacific Economic Cooperation (APEC). However, APEC's Privacy Framework is not binding on its signatory states, and thus does not have legal status for China.[141] More specifically, the CBPR system is a voluntary, accountability-based framework that serves to facilitate data flows across the APEC region, based on the APEC Privacy Framework. It is a government-backed data privacy certification system. The CBPR was endorsed by APEC Leaders in 2011. APEC members who want to join must demonstrate that they can enforce compliance with the CBPR system's requirements before joining. The Joint Oversight Panel (JOP) administers the APEC CBPR system. China, although acting as an APEC member economy, has never expressed any interest in joining as a member of this system. At present, Singapore and eight other APEC Member Economies are participating in the APEC CBPR system.[142] China is listed among the countries with which the Organisation for Economic Co-operation and Development (OECD) "works closely" within its scope of activities.[143]

With this said, in recent years, China has attempted to influence international data transfer rules and has promoted the concept of digital sovereignty. In September 2020, China announced the Global Data Security Initiative,[144] with a view to provide a framework for countries to cooperate on issues related to cross-border data flows. This Initiative is based upon three high-level principles, i.e., multilateralism,

---

[138] Article 4 of the Provisions on Regulating and Facilitating Cross-Border Flow of Data.
[139] Chorzempa and Sacks (n 135).
[140] Reuters, 'Exclusive: Shanghai to Allow Faster Data Transfer from China for Foreign Firms-Sources' <https://www.reuters.com/world/china/shanghai-allow-faster-data-transfer-china-foreign-firms-sources-2024-02-07/> accessed 19 February 2024.
[141] Graham Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?' (2004) 71 Privacy Laws & Business 16.
[142] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf
[143] https://www.oecd.org/about/members-and-partners/#:~:text=The%20OECD%20works%20closely%20with,the%20relevance%20of%20policy%20debates.
[144] 'Global Initiative on Data Security (全球数据安全倡议)' <http://www.gov.cn/xinwen/2020-09/08/content_5541579.htm> accessed 9 December 2022.

secure development, and fairness and justice,[145] together with eight more specific tenets.[146]

The Global Data Security Initiative has been seen as an avenue to build a larger framework for the global digital economy.[147] Since 2020, the Global Data Security Initiative has been mentioned by Xi Jinping in several summits, including the Shanghai Cooperation Organisation (SCO) Summit, the BRICS Summit, and the G20.[148]

At the regional level, China's recent position is reflected in its commitments to the Regional and Comprehensive Economic Partnership (RCEP) agreement.[149] Many of the RCEP provisions, for instance, on data localisation and cross-border data flows, reflect China's vision and preferences in terms of digital commerce, and are framed through the concept of digital sovereignty. The RCEP provisions on cross-border data flows thus provide more autonomy and flexibility to its signatories, when compared, for example, with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Under the RECP framework, signatories consent "not to prevent" cross-border transfers, allowing for varied measures if deemed "necessary" to attain a "legitimate public policy objective".[150] For instance, a footnote to Provision 12.14.3(a), which is the "legitimate public policy objective" exception, states: "[f]or the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party."[151] Notably, there is no stipulation mandating that the measure be the "least burdensome" for achieving the specified objective. Furthermore, the obligations are contingent upon an entirely self-determined and non-disputable national security exception.[152]

Similarly, by actively participating in the E-Commerce Joint Statement Initiative (JSI), China has pledged to propel those negotiations forward.[153] However, it has emphasised that security must be established as a prerequisite for the seamless flow of data across borders, a stance it has consistently taken in various multilateral forums, like the Baise Executive Leadership Academy, the China-ASEAN Information Port

---

[145] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative" 全球数据安全倡议' (*DigiChina*) <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 14 December 2023.

[146] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative" 全球数据安全倡议' (*DigiChina*) <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 14 December 2023.

[147] Hunter Dorwart, 'China and Global Data Transfers: Implications for Future Rulemaking' <https://papers.ssrn.com/abstract=4526107> accessed 14 December 2023.

[148] Park (n 146).

[149] Dorwart (n 147).

[150] Jones, E., Garrido Alves, D. B, Kira, B. and Sand, A. (2021) 'The UK and digital trade: which way forward?', Blavatnik School Working Paper 2021/038

[151] Felicity Deane and others, 'Trade in the Digital Age: Agreements to Mitigate Fragmentation' [2023] Asian Journal of International Law 1.

[152] Anna Sands and others, 'The UK and Digital Trade: Which Way Forward? | Blavatnik School of Government' (2021) <https://www.bsg.ox.ac.uk/research/publications/uk-and-digital-trade-which-way-forward> accessed 1 January 2024.

[153] https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

Forum, the China-Singapore Internet Forum, and the China-Africa Internet Development Cooperation Forum.[154]

5. Conclusions

As an important global player, China's digital economy has been continuously growing and expanding over the past 10 years. China is one of the most important trade actors in the world, holding significant partnerships with the EU, the US as well as the BRICS countries. Recognising the importance of safeguarding personal information, China has steadily built its data governance framework on three main pillars: the DSL, the CSL and the PIPL. The PIPL, which was enacted in 2021, serves as China's first comprehensive data protection law. Although highly influenced by the EU GDPR, the PIPL also contains many distinct features. The PIPL applies to "all kinds of information recorded by electronic or other means *related to identified or identifiable natural persons*" including sensitive personal information and biometrics data, while excluding anonymised data. Notably, PIPL also extends its subject-matter extraterritorially.

The cross-border transfer of personal information is regulated by Chapter III of the PIPL. The Chinese model for regulating data transfers is quite unique. Although the EU's influence on the Chinese data transfer regime is manifest, e.g. in the design of the Chinese Standard Contract, many provisions are China specific. These include a bespoke hierarchy of transfer tools and stringent data transfer restrictions targeting "CIIOs" and "important data".

China's regulations on cross-border data transfer aim to strike a balance between ensuring the "safe flow" and the "free flow" of data. That said, the implementation details of the regulated cross-border data transfer tools have not been fully unpacked yet. The first version of the cross-border data transfer regime is currently being reworked, in particular to address the needs of multinational organisations and cross-border e-commerce. Although a comprehensive data protection law, i.e., the PIPL, has been in force for two years, detailed guidelines are still evolving rapidly: the recent draft regulations can be seen as a move to try to preserve China's economic growth. [155] It has thus been argued that the Chinese cross-border data transfer regime is still in its infancy and will continue to evolve.[156] The recent evolution shows many inconsistencies and uncertainties in the interpretation and enforcement of these rules. The industry is calling for clearer definitions of key terms and more specific guidelines to make cross-border transfer rules easier to apply in practice. At the same time, local public entities are tempted to adopt more flexible rules.

Importantly, China's approach to data governance has been driven by the concept of digital sovereignty, which appears to be wide encompassing. China has thus been building a regulatory framework for cross-border data transfers to protect not only the rights of Chinese citizens and entities, but also to strengthen its capabilities to protect its cyber resilience and its national security interests.[157] On the global stage,

[154] Dorwart (n 147).
[155] Chorzempa and Sacks (n 135).
[156] Zhao (赵精武) (n 118).
[157] Yuan Li, 'Cross-Border Data Transfer Regulation in China' (2021) Rivista Italiana di Informatica e Diritto

China has been actively championing its vision in the context of several international initiatives, in particular by waving the digital sovereignty flag.[158] This proactive stance reflects China's commitment to shaping and contributing to international discussions and cooperation in the evolving landscape of global data governance, challenging competing jurisdictions to reassess their positions.[159] Nevertheless, translating China's domestic regulatory objectives into international standards remains a complicated task.[160]

<https://zenodo.org/records/5266546> accessed 15 December 2023.

[158] A detailed conceptualisation of digital sovereignty and its related tenets such as technology sovereignty, data sovereignty, national cyber resilience, national security, within the Chinese context, will be essential to inform discussions in international fora and build cooperation mechanisms for cross-border data flows.

[159] See for example the various proposals emerging in the US to redefine or refocus the US trade policy, e.g., S. Sacks and P. Swire, A framework for assessing US data policy toward China, June 2023 available at https://www.crossborderdataforum.org/a-framework-for-assessing-u-s-data-policy-toward-china/, accessed 1.1.24.

[160] Dorwart (n 147).

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

CROSS-BORDER DATA TRANSFER TOOLS V. PRIVACY ENHANCING TECHNOLOGIES: A FALSE DEBATE

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

Executive Summary

Privacy Enhancing Technologies (PETs)' potential has been acknowledged in various jurisdictions by data protection supervisory authorities. PETs have thus been prototyped in various sectors, in particular finance and healthcare, with the intention of generating new data flows. It is not surprising, therefore, to see that global efforts to promote the free flow of data across borders include workstreams on PETs. A framework to assess PET achievement, in particular in the context of cross board data transfers (CBDT), is however still needed. This paper aims to lay the foundations for the development of such a framework and thereby aims to inform the work done at the international level to reduce fragmentation of data transfer regimes, be it in the context of the G20, G7, or OECD initiatives.

CBDT tools are legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained, once the data is handled by the data importer operating in a third country, such as adequacy decisions, Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification. They are thus a means to produce evidence of trustworthiness: either institutional trustworthiness through the analysis of the legal framework applicable within the jurisdiction of the data importer, or relational trustworthiness through the assessment of the behaviour of the data importer or the formulation of binding commitments.

CBDT tools can be associated with at least two different types of data-transfer restriction patterns. A CBDT restriction pattern refers to a repeatable set of limitations imposed on the cross-border transfer of data from a data exporter to a data importer, which, through the requirement to adopt a data transfer tool, typically aims at exporting a certain level of data protection when the data leaves the jurisdiction in which it was initially processed or when the data is accessed from a third country. Restriction Pattern #1 targets the intended recipient of the transfer and aims to directly impact its processing practices. Restriction Pattern #2 targets the intended recipient and situationally relevant third parties, e.g., third parties who create additional risks to the fundamental rights of data subjects. This pattern aims to directly impact the processing practices of both groups. The best illustration of Restriction Pattern #2 is the solution that has emerged in the European Union (EU), following the Schrems II decision: whatever the CBDT tool at stake, either essential guarantees against abuses committed by public authorities when processing the personal data must exist or supplementary measures must be put in place to effectively mitigate against this threat.

A subset of PETs, called Confidentiality Enhancing Technologies (CETs), is an attempt to formalise the selection process of controls addressing confidentiality threats associated with unauthorised or unwanted access, which constitute the main threats to mitigate when considering situationally relevant third parties under Restriction Pattern #2. CETs, therefore, at least at first glance, appear particularly useful under Restriction Pattern #2. CET implementation implies adopting a fine-grained approach to data transfers, which is compatible with Restriction Pattern #2 and is not necessarily inconsistent with the EU model, for which there is leeway to move away from a one-size-fits-all approach. However, crucially, CETs do not eliminate trade-offs. They thus require careful consideration.

The paper includes a typology of CETs. It shows that each CET within this typology pursues a limited objective, and that CETs are not perfect substitutes in terms of the guarantee(s) they offer. Moreover,

following the inference model, it shows that whatever the CET at stake is, context controls (technical or organisational controls applied upon the environment of the data as opposed to the data itself) implemented within the data importer's perimeter will always be needed to address the full range of inferences (identify inference, attribute inference, participation inference, relational inference). Going further, it argues that anonymisation is always a trade-off, i.e. a decision to prioritise utility over confidentiality, even when the strongest CETs are in place.

From these findings, three consequences are drawn. First, the CET selection process should be made transparent, and assumptions related to the types of inference in scope and the threat model (where relevant) should be made explicit to allow oversight. Second, the full CET setting should be taken into account to assess the output, and in particular the legitimacy of the processing purpose once the data is in the hands of the data importer and the level of data subject or end user intervenability. This should hold true, even if a claim of legal anonymisation is successful, as the anonymisation process remains within the scope of data protection law. Third, even in the presence of CETs, relational trustworthiness remains relevant and CBDT tools will be needed to generate evidence.

This paper includes five recommendations for policymakers interested in setting or contributing to PET workstreams and who are engaged in actions to address the fragmentation of data flow regimes at the global level.

1. Introduction

Privacy Enhancing Technologies (PETs)' potential has been acknowledged in various jurisdictions by data protection supervisory authorities, including the European Data Protection Board (EDPB)'s predecessor.[1] PETs have thus been prototyped in various sectors, in particular finance and healthcare, with the intention of generating new data flows.[2] It is not surprising therefore to see that global efforts to promote the free flow of data across borders include workstreams on PETs.[3]

To facilitate convergences of approaches across regions while avoiding falling into the trap of

[1] Article 29 WP, Anonymisation Techniques, Opinion 05/2014 on Anonymisation Techniques, WP216, Adopted 10 April 2014. Guidelines on a similar topic have been produced in Canada, Singapore, Spain, the United Kingdom (UK). These guidelines however do not usually cover data transfer scenarios.

[2] See e.g., the UK FCC, Global AML and Financial Crime TechSprint, 2019, available at https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint, accessed 28.01.24; The UK-US PETs prize challenges, 2022-2023, available at https://www.ukri.org/blog/privacy-enhancing-technologies-pets-prize-challenges-winners/#:~:text=The%20PETs%20Prize%20Challenges%20have,both%20sides%20of%20the%20Atlantic accessed 28.01.24. Several use cases selected for prototyping PETs in the context of these initiatives however raise concerns as they could be classified as high-risk profiling.

[3] See e.g., UK Government, G7 Digital and Technology Track - Annex 2, 2021 available at https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf, accessed 28.01.24.

"technological solutionism",[4] it is essential to carefully unpack the potential of PETs in such a context.

The purpose of this paper is thus to lay the foundations for PET assessment in cross-border data transfer (CBDT) scenarios and include some recommendations for policymakers leading workstreams in the space. This brings us to introduce an intermediate category of PETs, to call for a fine-grained approach to data transfer, and stress that PETs should not be considered as mere substitutes to data transfer tools, i.e., legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained once the data is handled by the data importer operating in a third country such as adequacy decisions, Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification.

Cross-border transfer tools can be associated with at least two different types of data-transfer restriction patterns. A CBDT restriction pattern refers to a repeatable set of limitations imposed on the cross-border transfer of data from a data exporter to a data importer, which, through the requirement to adopt a data transfer tool, typically aims at exporting a certain level of data protection when the data leaves the jurisdiction in which it was initially processed or when the data is accessed from a third country. Restriction Pattern #1 targets the intended recipient of the transfer and aims to directly impact its processing practices. Restriction Pattern #2 targets the intended recipient and situationally relevant third parties, e.g., third parties who create additional risks to the fundamental rights of data subjects, and aims to directly impact the processing practices of both groups.

Although Restriction Pattern #2 is per definition more demanding than Restriction Pattern #1 in terms of the types of controls one would need to put in place to protect the data, this does not mean that Restriction Pattern #2 is inherently flawed and does not lend itself to a formalised risk-based assessment. A subset of PETs, called Confidentiality Enhancing Technologies (CETs), is an attempt to formalise the selection process of controls addressing confidentiality threats associated with unauthorised or unwanted access, which constitute the main threats to mitigate when considering situationally relevant third parties under Restriction Pattern #2. Their implementation implies adopting a fine-grained approach to data transfers, which is compatible with Restriction Pattern #2. Crucially, however, implementing such CETs should not mean that the data exporter is given carte blanche to initiate the transfer and that there is no need to subject the data importer to additional restrictions.

A data transfer tool will still be needed at a minimum to ensure that context controls, i.e., controls applied upon the environment of the data such as purpose-based access control, have been put in place within the perimeter under the data importer's responsibility. This is because, even if CETs, in some instances, would make it possible to achieve legal anonymisation, i.e., to reduce re-identification risks to an acceptable level, such a finding cannot be made upon the consideration of the data control applied on the data only, i.e., the data transformation technique applied on the data. Going further, as an anonymisation finding is always a trade-off, i.e., a decision to preserve utility over confidentiality, such a trade-off should

[4] To use Morozov's expression coined in his 2011 book. E. Morozov, The Net Delusion: the Dark Side of Internet Freedom, 2011, PublicAffairs.

always be validated at a minimum in the light of the legitimacy of the downstream processing purposes and the level of data-subject or end-user intervenability allowed by the CET setting. What is more, considering the CET setting holistically and bearing in mind that the anonymisation process remains governed by data protection law, the data exporter should select the CET setting that preserves the highest level of data subject intervenability.

This paper is structured as follows. Section two introduces the two main data-transfer restriction patterns that are found in practice. Section three unpacks the potential of CETs in the context of data transfers and highlights their implications and limitations. Section four concludes.

2. Data-Transfer Restriction Patterns

Two main data transfer restriction patterns usually emerge when reviewing data transfer regimes.

2.1. Restriction Pattern #1: "Bind the Intended Recipient"

The primary objective of a CBDT mechanism is to define a normative baseline with which the data importer must comply, i.e., to bind the intended recipient of the data when operating within its own jurisdiction to ensure a pre-determined level of data protection. This is what is called Restriction Pattern #1. The focus of this pattern is set upon the intended recipient: it is therefore (e.g., contractually) imposed a series of obligations such as obligations related to purpose limitation, data minimisation, record keeping, security (integrity and confidentiality) and breach notification, and individual right-related obligations.

The normative baseline can also include rights granted to third-party beneficiaries, who are thus empowered, at least as a matter of principle, to enforce their rights against the parties to the CBDT. Third party beneficiaries' rights can cover a wide range of obligations imposed upon data importers, e.g., provisions that provide safeguards for the handling of personal data or ensure specific individual rights.[5]

Unsurprisingly, the strength of the normative baseline embodied within CBDT mechanisms can vary greatly. To take the example of model clauses, the ASEAN model contract clauses, for example, have very little on third-party beneficiary rights, as they are designed to enforce safeguards mandated within the ASEAN Framework on Personal Data Protection of 2016. On the other hand, the Ibero-American Model Transfer Agreement aims to enable entities to meet the Personal Data Protection Standards for the Ibero-American States: it is therefore closer to the EU Standard Contractual Clauses (SCCs). Its goal is to ensure that "the level of protection of the personal data of the citizens of a country does not decrease or disappear when exported or transferred to another country or countries."[6] Of note, although Brazil

[5] The best example is the set of model clauses developed by the European Union (EU). See 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 (Text with EEA relevance) C/2021/3972 OJ L 199, 7.6.2021, p. 31–61.

[6] Ibero-American Data Protection Network, Annex Model Contractual Clauses, p. 13, March 2023, available at https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-

includes model clauses within its transfer toolbox, it has not yet endorsed this set of model clauses, as it is probably waiting to receive an adequacy finding from the EU first.

Importantly, and as mentioned above, when the restriction pattern at stake is Restriction Pattern #1, data handling obligations are usually imposed upon the data importer. Imposing data handling obligations upon the data importer should imply on the part of the data importer an obligation to implement controls to prevent confidentiality threats such as unauthorised access. As the intensity of the controls should be proportionate to the risks posed to data subjects, a risk assessment should be performed by the data importer even when Restriction Pattern #2 is not applicable. This does not mean however that the threat model that the data importer should be using to select appropriate controls and comply with its obligations will necessarily include public authorities.[7] In fact, standard practice, as described by Data Protection Authorities, such as the UK Information Commissioner's Office (ICO), excludes public authorities from the definition of a typical motivated intruder.[8]

It is worth noting that Restriction Pattern #1 can emerge even in scenarios in which there is no express CBDT rules issued by the jurisdiction of the data exporter. Suffice it to identify a requirement to bind the data recipient even when data handling rules are not applicable to the latter as a covered entity. This is what happens with the California Consumer Privacy Act, as amended by the California Privacy Rights Act, since it includes a requirement to bind service providers through contract and specifies a minimum set of obligations to include within such a contract.[9]

2.2. Restriction Pattern #2: "Bind the Intended Recipient and Shield against Third Parties"

Restriction Pattern #2 has a broader target than Restriction Pattern #1. It aims to impact both the practices of the intended recipient and third parties that are situationally relevant, such as public authorities.

Let's take the example of a specific data transfer tool to better illustrate Restriction Pattern #2 and compare it with Restriction Pattern #1: the EU SCCs.[10] The roots of Restriction Pattern 2 associated with

---

en.pdf, accessed 28.01.24.

[7] " Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value," e.g. data as OWASP explains. "A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device)." OWASP, Threat Modelling, available at https://owasp.org/www-community/Threat_Modeling, accessed 28.01.24. An event is usually associated with a particular attacker, for whom a series of assumptions will be made to define its profile.

[8] See ICO, Code of Practice on Anonymisation, 2012, available at https://ico.org.uk/media/1061/anonymisation-code.pdf, accessed 28.01.24 and the 2022 draft chapters produced to revise the 2012 Code available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/, accessed 28.01.24.

[9] See California Civil Code section 1798.100(d).

[10] On 4 June 2021, the EU Commission adopted the latest version of SCCs through it Implementing Decision (EU) 2021/914 and thereby replaced the set of clauses adopted under the Data Protection Directive and before the CJEU's Schrems I and II rulings. By doing so, it introduced four modules to govern four different types of relationships: transfers from data controller to data controller, data controller to data processor, data processor to data processor,

the EU SCCs, are to be found in two places. First of all, Article 44 of the General Data Protection Regulation (GDPR)[11] states that "[a]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."[12] Article 44 must be read in the light of Article 46(1)[13] and Article 46(2).[14] There are at least two ways to interpret these provisions together: either the use of SCCs creates the presumption that data subjects have been granted effective rights on the condition that the rights are enforceable under the law of the contract,[15] or the SCCs do not create any conditional presumption. Excluding the first interpretation would clearly undermine the raison d'être of EU SCCs. As of today, there is no reason to exclude this interpretation. The EC's 2021 decision acknowledges that with these new international transfer SCCs, the parties can freely choose the EU Member State law that will govern their SCCs, on the condition that the Member State's laws allow for third-party beneficiary rights.[16] The Court of Justice of the European Union (CJEU) in Schrems II made it clear that appropriate safeguards are able to be provided by the SCCs adopted by the Commission.[17]

The second locus of Restriction Pattern #2, as embodied in EU SCCs, is to be found in the Charter of Fundamental Rights of the European Union (Articles 7, 8, 47 and 52). This has been confirmed by the CJEU, and in particular in its Schrems II decision specifically examining the validity of SCCs.[18] This led the CJEU to state that *"the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data*

---

and data processor to data controller. All transfer tools should be associated with the same restriction pattern.

11 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) OJ L 119, 4.5.2016, p. 1–88.

12 GDPR, Article 44.

13 Article 46(1) provides that: "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

14 Article 46(2) provides that: "The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:...(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)."

15 In order to achieve effective enforcement, the data importer through the SCCS agrees to submit itself to the jurisdiction of the competent supervisory authority (usually the competent supervisory authority of the EU Member State in which the data exporter is established), to cooperate with such authority and comply with any binding decision under the applicable EU or Member State law, including decisions rendered by an EU Member State's court. Data subjects also get a right to access SCCs.

16 Ireland had been the only member state that did not allow for third-party beneficiary rights as the law had required strict privity of contract. Despite some commentary about data subjects being able to use a theory of agency to enforce their rights, the Irish Department of Justice issued a statutory instrument to amend the Irish Data Protection Act 2018.

17 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. 2.

18 Schrems II, para. 105.

transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."[19]

What the CJEU is thus suggesting in Schrems II is that in certain cases public authorities should be considered as situationally relevant attackers. To determine whether the public authorities of the third country should be considered situationally relevant attackers, an assessment of the legal system of the third country is considered to be necessary by the CJEU. More specifically, both a legal analysis and a factual analysis appear to be in scope, as the CJEU refers to relevant aspects of the legal system of the third country.[20] This is because access by public authorities is dependent upon the scope of interception powers and powers to request access to data held by private parties as well as the practice of these powers.

The CJEU goes further, however, when it imposes upon data controllers an obligation *"to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned."*[21] Following its Advocate General, the CJEU holds 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."*[22] Although such a stance could appear harsh to data exporters at first glance, the presumption of responsibility imposed upon the data controller is a general underpinning of the GDPR, as illustrated by Article 82(2), which aims at ensuring that data subjects are granted an effective right to compensation. Importantly, such a stance does not preclude Supervisory Authorities, the European Data Protection Board (EDPB), nor the European Commission, to become more proactive and produce their own legal assessment with a view to alleviate the burden imposed upon data controllers.

In an attempt to offer detailed guidance to data exporters, the EDPB produced a set of recommendations on supplementary measures which includes an assessment method.[23] This method comprises a requirement for data exporters to produce a legal analysis, as well as an analysis of public authorities' practices. The upshot of such an analysis should in theory help data controllers determine whether supplementary measures are needed, i.e., measures reasonably likely to mitigate against confidentiality threats posed by public authorities.

Given the powers and means of public authorities, it is reasonable to assume that context controls, including technical controls affecting the environment as opposed to the data itself, such as access controls, cannot suffice. Data controls such as de-identification and anonymisation techniques thus appear to be key controls in this context. This explains the focus upon PETs, or at the very least, a subcategory of PETs.

---

[19] Schrems II, para. 105.
[20] Schrems II, para. 126.
[21] Schrems II, para. 142.
[22] Schrems II, para. 134.
[23] 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.

3. PETs as Supplementary Measures

The EDPB has made it clear that PETs could be useful measures in the context of CBDTs to help justify the lawfulness of the transfer. [24] Commentators have however been very severe with the EDPB's recommendations on supplementary measures even if the second version of the recommendations appears less restrictive than the first one. Rubinstein and Margulies write for example that "[w]hile the Final Recommendations identify risk-based factors for evaluating foreign law and the effectiveness of supplementary measures, in the end these factors reduce to the binary decision of whether or not the essential equivalency standards are satisfied."[25] For the purposes of this note, the difficulty stems from the fact that it is confusing to acknowledge the relevance of PETs without clearly unpacking a risk-assessment method. Yet, the EDPB does not specify a risk-assessment method that could be leveraged for the selection of PETs.

To lay the foundations for such a risk-assessment method, it is important to build a PET typology, organising PETs by objective and limitation. Once this is done, it becomes clearer that PET selection implies a fine-grained approach to data transfer and that PETs cannot act as substitute for data transfer tools.

3.1. A PET typology

Relevant PETs

The ICO defines PETs as "technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and/or empowering individuals. Data protection law does not define PETs. The concept covers many different technologies and techniques."[26] The European Union Agency for Cybersecurity (ENISA) refers to PETs as:" software and hardware solutions, i.e. systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons."[27]

What these definitions do not make clear is that PETs can be of relevance for any type of confidential data, be it personal or not.[28] This is the reason why the concept of CETs is introduced. CETs, a subset of PETs,[29]

---

[24] EDPB, Ibid.

[25] 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, 443.

[26] ICO, Draft Chapter 5: Privacy Enhancing Technologies, September 2022, p. 3.

[27] See also the 2023 UN PET guide available at https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf, accessed 28.01.24; the Royal Society, From Privacy to partnership - the role of privacy enhancing technologies in data governance and collaborative analysis, Policy Report, January 2023, available at https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf, accessed 28.01.24.

[28] See e.g., the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, which calls for implementing appropriate data input measures and protections for personal data and intellectual property, available at https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems, accessed 28.01.24.

[29] There is a long history of using PETs to engineer data protection requirements within IT systems. PETs are usually

are an attempt to formalise the selection of controls for a given (and limited) type of threats, i.e., confidentiality-related threats associated with unauthorised or unwanted access. CETs, just like PETs in general, are not a means to address all data protection goals at once.[30] In fact, their implementation usually embed a variety of trade-offs between competing data protection goals (usually determined in the light of business interests pursued), e.g., typically between confidentiality and transparency, or even between confidentiality and fairness. [31] Such trade-offs, it is suggested, should always be made explicit when a CET is selected for a particular use case, bearing in mind that duties to preserve data-subject or end-user intervenability through appropriate design are starting to emerge more clearly.[32] These duties are all the more relevant that any personal data transformation process is subject to data protection law, including anonymisation processes.

Importantly, CET settings can vary greatly. In some cases, they will rely upon a trusted intermediary, in others they make it possible to bypass trusted intermediaries. In some cases, they are set up directly between the data subject and the intended recipient of the data, in others they are set up between a controller and a processor or a covered entity and a service provider or contractor.

In the context of Restriction Pattern #2, when situationally relevant third parties are in scope, one is concerned with a specific confidentiality threat, which should be mitigated through the prevention of unwanted access.

The list of potentially relevant CETs in such a context is represented in Table 1:

CET	Goal
Global Differential Privacy (GDP)	GDP ensures that an attacker querying the data set cannot reliably infer whether a particular individual's data is included within the data set, even with access to every record in the data set, except for that specific individual's data.
Local Differential Privacy (LDP)	LDP ensures that an attacker querying the data set cannot reliably infer whether a particular attribute is associated with a particular individual whose data is included within the data set,

understood broadly and span a variety of coded safeguards, including consent management processes or cookie banners.

[30] Engineers often reduces data protection or privacy to confidentiality. See e.g., S. Gürses, Can You Engineer Privacy? (2014) 57 Communications of the ACM 20.

[31] See e.g., e.g. M. Veale, Denied by Design? Data Access Rights in Encrypted Infrastructures, 2023, July 27, available at https://doi.org/10.31235/osf.io/94y6r, accessed 28.01.24 ("Designing privacy into complex informational infrastructures requires the navigation of trade-offs that do not have an intuitive or obvious balance.")

[32] See e.g. in relation to data access by users of connected products Recital 20 and Article 3(1) of the EU Data Act ("Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user").

	even with access to every record in the data set, except for that specific individual's data.
K-anonymisation (K-anon)	K-anonymisation ensures that an attacker with access to the data cannot single out a particular individual within the data set beyond a minimum k number of records
Homomorphic Encryption (HE)	HE ensures that an attacker, including a malicious processor, cannot access the input data it computes over and the results it generates form the computation.
Trusted Executive Environment (TEE)	TEEs ensures that an attacker, including a malicious processor, cannot access the input data it stores.
Federated Learning (FL)	FL ensures that a Machine Learning (ML) architecture processes user-level training data locally and send model outputs only to a centralised server.
Secure Multi-Party Computation (SMC)	SMC ensures that a participant to the scheme cannot access the raw data held by other participants to the scheme.
Zero Knowledge Proof of Knowledge (ZKPK)	ZKPK is a special case of SMC, that allows a user to prove an assertion without revealing any confidential information related to the assertion.
Synthetic Data	Synthetic data is drawn from a model which has been trained on real data and which outputs data such that it is considered to be consistent with the training data.

Table 1. CET goals

The Inference Model

There are different ways confidentiality threats can be mitigated, and the choice of controls should ultimately depend upon the type of inference to prevent.

The inference model is a formalised method developed to inform confidentiality-related risk assessment.[33]

In an inference model, there are four types of inferences an attacker could try to make:

[33] S. Stalla-Bourdillon & A. Rossi, Aggregation, synthesization and anonymization: a call for a risk-based assessment of anonymization approaches, in Data Protection and Privacy, Volume 13: Data Protection and Artificial Intelligence ed. D. Hallinan, R. Leenes, & P. de Hert , Hart Publishing (2021), chap. 5.

1. Identity inference: inference that a record corresponds to an individual.
2. Attribute inference: an inferred value for a particular attribute within an individual record.
3. Participation inference: an inference that the data of a particular individual is included within a data set.
4. Relational inference: an inference that two records correspond to the same individual.

Because CETs are built to achieve a very limited objective, it is hard to compare them. It is however possible to distinguish between the following five objectives, which should inform the choice of the best-suited CET for a given use case:

1. To offer a guarantee of deniability to the participant to a data set. In other words, once the CET is applied it will be possible to argue that a particular data subject or data point has never been included in the data set and therefore data associated with the data subject or data point could not have contributed to the query results.
2. To offer a guarantee of deniability as to the value of particularly sensitive attributes. In other words, once the CET is applied it will be possible to argue that a participant to the data set has never been associated with a particular sensitive value or that a particular event or product has never been associated with a particular sensitive value.
3. To offer the guarantee that the raw data has never been accessed by a particular stakeholder, which is different from stating that no inference has ever been derived from the raw data.
4. To offer the guarantee that it is not possible to single out an individual, an event or a product within a particular data set, which is different from arguing that it is not possible to infer any attribute, including a sensitive attribute, about a particular individual or product or service.
5. To offer the guarantee that an untrusted processor cannot read the protected data, which is different from stating that the data holder cannot compute over the protected data, although the processor will not be able to read the results of the computation either.

Each CET usually addresses one of these objectives. Some CETs offer formal guarantees,[34] others do not.

Crucially, CETs should not be examined in isolation but should be assessed within their settings. A CET setting has three main components: data (input and output data), stakeholders (at a minimum a data exporter and a data importer), and infrastructure (technical and organisational structures that make processing by the data importer possible). CETs, irrespective of the formal guarantee they offer, always require the implementation of context controls once the broader picture of the CET setting is taken into

[34] A formal guarantee is a guarantee that can be demonstrated mathematically.

consideration.[35] Given the limited guarantee they offer, it may make sense to combine them.[36]

In a non-data transfer scenario, where public authorities are not arguably in scope, a situationally relevant attacker is usually defined in terms of a motivated intruder who does not have prior knowledge and does not necessarily possess expert technical skills.[37]

In a non-data transfer scenario, the inference model leads to a risk-based assessment centred around the following questions:

1. Is it reasonable to assume that the main inference to mitigate against is identity inference? (Note that identity inference is usually associated with objective 4)

2. Given the sensitivity of some attributes at stake, would it make sense, as a matter of precautionary measure, to mitigate against attribute inference as well? (note that attribute inference is usually associated with objective 2)

3. Given the sensitivity of group membership-related information, would it make sense, as a matter of precautionary measure, to mitigate against membership inference as well? (Note that group membership inference is usually associated with objective 1)

4. Given the data environment at stake, does it make sense as a precautionary measure to also mitigate against the linking of certain types of data sets?

Often, in practice, the answer to the first question is positive. On occasions, some additional data controls are put in place to mitigate against sensitive attribute inference or group membership inference as well. Relational inference may be of relevance, for example, when data is combined in such a way that it would very easily jeopardize mitigation against identity inference.

Crucially, it is not possible to completely eliminate re-identification risks and even when identity inference risks are mitigated to a satisfactory level, other types of confidentiality-related risks can persist.[38]

Going further, unless one implements a data transformation method that is indifferent to the attacker's prior knowledge or one precisely determines the extent of an attacker's prior knowledge, it is simply impossible to rule out inference attacks in the absolute sense.[39] It follows that simplistic oppositions drawn between individual-level data and aggregated data are misleading.[40] It is just wrong to claim that relying upon aggregated data never raises privacy concerns. A better formulation would be to state that anonymisation can be pursued through the aggregation route but is likely to require more than

[35] S. Stalla-Bourdillon & A. Rossi, n(33).
[36] S. Stalla-Bourdillon & A. Rossi, n(33).
[37] See ICO, Code of Practice on Anonymisation n(8), and the 2022 draft chapters n(8).
[38] In particular, when the attacker has some prior knowledge.
[39] C. Dwork, Differential Privacy, Lecture Notes in Computer science book series, LNTCS, volume 4052.
[40] See e.g., the European Commission's statement in the EU-US 2023 adequacy decision: "Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns."

aggregation to mitigate re-identification risks.

Basically, a controller is thus left with two options: either to minimise the amount of information transmitted to a potential attacker regardless of the background knowledge of the attacker through the formalisation and implementation of global differential privacy-based controls (option 1) or to formalise an attack model (i.e., drawing a realistic profile of the situationally-relevant attacker) and implement relevant controls arguing that either it is reasonable to assume that any attacker successful in reaching the data is unlikely to possess relevant background information, or that when such an event occurs, individual impact is limited by the applied controls (option 2). To be truly indifferent to the background knowledge of the attacker, option 1 requires implementing a privacy budget for each data consumer, which when exhausted, will mean that the data consumer will not be able to query the data further. What this means is that access control, i.e., a context control, is essential for the success of option 1.

As a result, anonymisation always remains a trade-off, i.e., a decision to prioritise utility over confidentiality. Therefore, anonymisation should always be coupled with safeguards applicable to downstream uses: in particular, it is essential to make sure that the purpose for which the data is anonymised is legitimate and to consider whether some level of data-subject or end-user intervenability is preserved. Interestingly, the recently adopted Quebec Law 25, which amends the Act respecting the protection of personal information in the private sector,[41] acknowledges the importance of purpose legitimacy clearly. What is more, it is possible in practice to set up CETs in such a way that data lineage, and therefore capabilities to object, are preserved, even if data is transformed to reduce re-identifiability risks for a particular use case.

Recommendation: Consider showcasing CET settings that are able to preserve data-subject and end-user intervenability.

To be sure, even if anonymisation is fundamentally a trade-off, resorting to threat modelling techniques is not pointless. It is actually quite the opposite: these techniques force the data controller to make its assumptions explicit. Yet, we suggest that both assumptions related to the types of inference in scope and the applied threat model should be made explicit to allow oversight.

Recommendation: Consider producing guidance on threat modelling techniques.

Data Transfers and PETs

In the context of data transfers, public authorities comprising intelligence services and law enforcement agencies representing situationally relevant attackers should be assumed to have prior knowledge and

[41] chapter P-39.1, Section 23 (”Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information, or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act”).

expert technical skills: global differentially private methods (i.e., option 1) thus appear more attractive. However, when this option is not available due to utility constraints, an attack model will need to be formalised (i.e., option 2), which will imply making assumptions about the degree to which the data would be of interest to the situationally-relevant attackers or would otherwise already be available to them, and the types of individual impact (e.g., which could be a physical or psychological harm or even a human-right violation) a successful attack could generate.

The strongest CETs or combination of CETs in a CBDT context appear to be:

CET	Guarantee (under a suitable attack model)	Effect	Limitation
GDP	Formal deniability against participation	Prevents an attacker from learning more than a limited amount of additional information about an individual record (the amount is controlled by E)	The mathematical value Epsilon (often named privacy budget) is set properly
K-anon + LDP	Formal guarantee against singling out Formal deniability against sensitive attribute disclosure	Prevents an attacker from attributing a record to an individual Prevents an attacker from learning more than a limited amount of additional information about an individual's attribute	Both the mathematical values Epsilon (often named privacy budget) and K (the number of individuals sharing identical attributes within a data set) are set properly
HE	Formal practical impossibility to read the input data and the results	Prevents an attacker from learning non-negligibly more than the message length in practice	Decrypting without the key is computationally infeasible
TEE	Formal practical impossibility to read the input data (no guarantee for the results unless other protective measures are put in place)	Prevents an attacker from learning non-negligibly more than the message length in practice	The hardware manufacturer is trusted, the hardware is bug free and not under physical surveillance, and the PKI is trusted
SMC	Formal practical impossibility to read the	Prevents an attacker from accessing the data when	Decrypting without the key is (at least) computationally

	input data of other party members (but no guarantee for the results unless other protective measures are put in place)	jointly processing the data (but the attacker could learn anything inferable from the size of the input together with the results)	infeasible
Note on FL: There is no guarantee as FL is an ML architecture which has the effect of minimising the amount of data processed by the global model with no guarantee that the global model cannot memorize the training data.[42] However, FL can be coupled with differentially private techniques. Note on Synthetic Data: There is no guarantee as Synthetic Data is simply the product of a model that is trained to reproduce the characteristics and structure of the original data with no guarantee that the generative model cannot memorise the training data.[43] However, data synthetisation can be coupled with differentially private techniques.			

Table 2. CETs that may be relevant in a cross-border data transfer context

Again, as it is not possible to eliminate all re-identification risks, anonymisation in the context of data transfers remains a trade-off, despite the absolutist language used by the EDPB[44] who seems to ignore that the absolute impossibility to attribute the information to an individual can only be based upon the information available within the data set under GDPR Article 4(5). Yet, once both publicly available information and prior knowledge are in scope, it becomes impossible to ensure such an absolute … impossibility! This therefore means that the processing purpose should remain a key component of the assessment, as well as the level of data-subject or end-user intervenability preserved, and that there may be an argument to loosen restrictions when transfer is in the public interest. By way of example, this

[42] To be more precise, FL does not make it possible to guarantee that the data shared under FL is only the data needed to fulfil the learning task. T. Stadler, B. Kulynych, N. Papernot, M. Gastpar, C. Troncoso, The Fundamental Limits of Least-Privilege Learning, 19 February 2024, arXiv:2402.12235 [cs.LG].

[43] See Stalla-Bourdillon & Rossi n(33); Georgi Ganeve, Emiliano De Cristofaro, On the inadequacy of similarity-based privacy metrics: reconstruction attacks against "Truly Anonymous Synthetic Data", 8 December 2023, arXiv:2312.05114 [cs.CR].

[44] The EDPB states that to make pseudonymisation an effective supplementary measure, "a data exporter [must] transfer personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject." EDPB, Recommendations n(23), para. 85. This absolutist language comes from the definition of pseudonymisation in the GDPR and seems to suggest that the EDPB is only concerned by identity inference, which does not really align with prior guidance on anonymisation techniques. Used in the context of the recommendations, this language seems to imply that pseudonymisation is more protective than anonymisation, which makes little sense unless the EDPB is endorsing the option that is presented in the next paragraph, which is rather uncertain.

would explain why Article 6(11) of the EU Digital Markets Act foresees the possibility to produce anonymised data related to user queries inputted into search engines to the benefit of third-party search engines that are not gatekeepers.[45]

Pushing the analysis further, the difference in the range of situationally-relevant attackers between a non-transfer scenario and a transfer scenario means that data that is considered anonymised within the EU should not necessarily be authorised to travel to third countries, as additional checks may be needed to ascertain whether the data should be considered appealing to a wider range of situationally-relevant attackers, i.e., intelligence services and law enforcement agencies, and whether sensitive information has been protected to an acceptable level. One way to eliminate this double standard would be to assume that in a data transfer context, the output data remains at most pseudonymised. This would make it possible to govern onwards transfer while not necessarily ruling out data transfers. Note that the ICO is of the view that it is possible to achieve anonymisation in the hands of the data importer.[46]

As it is becoming clear from this analysis, implementing CETs implies a trade-off and can be resource intensive. One way to reduce uncertainty would be for a competent authority, e.g., the EDPB at the EU level, to produce clear guidance about the types of legitimate use cases CETs could enable in a data transfer context. This would not necessarily relieve data exporters from their risk assessment obligations however, as they would focus the analysis upon the particular implementation of the CET within a pre-determined setting and assess the limitations of the CET in this context.

When assessing CET use cases to select legitimate ones, it is essential that CETs' implications in terms of data and infrastructure monopoly be seriously taken into account to avoid strengthening monopolies through CET promotion,[47] which explains why imposing a blanket obligation to use hard PETs[48] on the ground of a data protection-by design obligation only, such as GDPR Article 25, remains problematic.[49] At

[45] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022, p. 1–66. See also S. Stalla-Bourdillon and B. Da Rosa Lazarotto, Search queries and anonymisation: How to read Article 6(11) of the DMA and the GDPR together?, European Law Blog, 3 April 2024, available at https://europeanlawblog.eu/2024/04/03/search-queries-and-anonymisation-how-to-read-article-611-of-the-dma-and-the-gdpr-together/, accessed 1.5.24.

[46] ICO, Annex to the Transfer Risk Assessment Tool, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/#TRA-tool, accessed 28.01.24. ("Note: You should also consider anonymisation techniques. If the personal information is effectively anonymised in the hands of a receiver so that it is no longer personal information, the UK GDPR transfer").

[47] See e.g., E. Renieris, Why PETs (privacy-enhancing technologies) may not always be our friends, How privacy-enhancing technologies can exacerbate rather than ameliorate technology and data governance concerns, Blog post 2021, available at https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/, accessed 28.01.24; M. Veale, Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!, 2023, SocArXiv. August 1. doi:10.31235/osf.io/4ugxd.

[48] an expression sometimes used to refer to CETs or a subpart of CETs.

[49] See e.g., I. Rubinstein and N. Good, The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default (September 30, 2019). International Data Privacy Law (2020) doi: 10.1093/idpl/ipz019, who argue that "In order to advance data protection in its own right rather than merely reinforce the general principles

most, an obligation to consider the implementation of CETs could be imposed but it would need to be clear that in some setting a resource-intensive process will have to be implemented to iteratively address competing data protection goals such as confidentiality and fairness.[50]

Recommendation: Consider producing a list of recommended PET use cases starting with use cases that are in the public interest considering a wide range of dimensions of concern.

3.2. Fine-grained Data Transfer Assessment

To be able to formalise an attack model, a fine-grained assessment of the data transfer at hand is necessary. A fine-grained data transfer assessment implies distinguishing between different types of processing activities on the basis of the level of data sensitivity, data availability, anticipated individual impact if situationally relevant attacks succeed, the legitimacy of processing purposes and the level of data subject or end-user intervenability. Such an approach, however, does not align well with the one-size-fits all approach adopted by some EU data protection authorities, which quite understandably have been wary of data exporters' attempt to perform risk assessments in this context.[51] This said, these authorities have more leeway than they think.

One concern usually raised when a fine-grained approach to data transfer is presented relates to the subjectivity of the assessment, which may undermine the Schrems II holding.[52] There are however ways to address such a concern. The most effective way would probably be for a competent authority sitting within the jurisdiction of the data exporter to expressly acknowledge that public authorities, i.e.,

---

of the GDPR, Article 25 must be interpreted as requiring the implementation of privacy engineering and hard PETs. A bold way to achieve this is by mandating that data controllers use available hard PETs for data minimisation."

[50] S. Stalla-Bourdillon, A. Rossi and G. Zanfir-Fortuna, Data Protection by Process - How to Operationalize Data Protection by Design for Machine Learning, FPF and Immuta White Paper, 2019, available at https://www.immuta.com/resources/data-protection-by-process-fpf-whitepaper/, accessed 1.5.24. In some cases, differential privacy, when homogenising training data, may negatively impact a minority group often defined by a protected characteristic. In other cases, minority groups could however be positively impacted by the homogenisation process. It is thus important to consider the impact of the CET on the outcome when training a machine learning model and any relevant notions of fairness should be included in the assessment to set an appropriate tradeoff between confidentiality and fairness during the different stages of the training phase.

[51] For a critique of these decisions see Lokke Moerel, What happened to the Risk Based Approach to Data Transfers? How the EDPB is rewriting the GDPR, (Future of Privacy Forum blog, 2022). This author, however, does not unpack the concept of a risk-based approach. See also on a risk-based approach to data transfer requirements Paul Breitbarth, A Risk-Based Approach to International Data Transfers, EDPL, 2021, p. 547; Christopher Kuner, Schrems II Re-Examined (VerfBlog, August 25, 2020), available at https://verfassungsblog.de/schrems-ii-re-examined/ accessed 28.01.24; and C. Kuner, L. Bygrave and C. Docksey, The EU General Data Protection Regulation: A Commentary, Update of Selected Articles, Oxford University Press, 2021, p. 113.

[52] This seems to have worried the EDPB in particular who in its first version of its recommendations had stated that data exporters shall "not rely on subjective [factors] such as the likelihood of public authorities' access to your data in a manner not in line with EU standards." EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 1.0, Adopted on 10 November 2020, para. 42.

intelligence services and law enforcement agencies are not interested in all types of data, and exclude low-risk data, starting with data that could easily be accessed through other means, unless the scope of the database would be such that it would offer an added-value to the third-party attacker, e.g., a social media data base. The US Government 2020 White Paper for example states that "[c]ompanies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."[53] While more granularity would be preferable, it is probably fair to infer from this statement that business-to-business personal data or personal data collected in the context of business-to-business relationships, which usually comprises names, job titles, and contact details, (that is to say a reduced set of demographic data) and is information that is usually publicly available on a variety of platforms, be it social media or businesses' own websites, should be considered low risk in a data transfer context.

Telemetry data is another category of data that is often discussed in the context of CBDTs.[54] Telemetry data usually includes sessions, events, logs that are generated by an application. There are however two types of telemetry data that are worth distinguishing: system telemetry data, which is often used for security purposes, and is first and foremost interested in the behaviour of an application. Some items of personal data could nonetheless be present in the logs generated by the application such as IP addresses, emails and/or account names, permission and/or access grants... User telemetry data, which tends to be used for product and service improvement, concerns the way users use the services. It usually comprises user ids, which could be randomised or at the very least obfuscated, device information, clicks within the product or service, and other actions. There is often no need to process directly identifying user telemetry data, but user telemetry data could potentially encompass a wide range of activities, in particular when joined across products and services before being aggregated at some later point in time. Notably, in an AI context, user telemetry is likely to include prompts or input data. There are good arguments for compromising on the flow of system telemetry data. They comprise a limited set of personal data that is shared with the service provider running the application for a legitimate internal purpose: to guarantee that the application is secure.[55]

---

[53] US Government, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, White Paper, September 2020, available at https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF, accessed 28.01.24.

[54] See e.g., Ministry of Justice and Security, Government of the Netherlands, DPIA report diagnostic data processing in Microsoft Office 365 for the Web and mobile Office apps (report delivered March 2020, Update June 2020) available at https://open.overheid.nl/documenten/ronl-aba85735-5a7a-4a8c-9c7a-7755d6bef118/pdf, accessed 28.01.24; Portugal National Data Protection Commission, Deliberation 1072/2022, available at https://www.cnpd.pt/decisoes/deliberacoes/, accessed 28. 01.24.

[55] See also P. Swire et al., Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics and Procedures, Draft June 1, 2023, available at https://ssrn.com/abstract=4466479, accessed 28.01.24, who argue on the basis of the EDPB's guidance on breach notification that "in most contexts the data elements used in cybersecurity, such as IP address, MAC address, or email address, are low risk – not requiring a breach notice even when they are seized illegally by hackers and transferred to a third country." The position taken in this paper is

Interestingly, the European Commission itself in its adequacy decision concerning the US indirectly acknowledges that certain types of human resources data are less risky than other types of data, or said otherwise, tries to find a compromise for data processed for occasional employment-related operational needs.[56] This solution should also be seen in the light of the EDPB guidance on the definition of restricted transfers within the meaning of Chapter V, which excludes from its remit data flows between individual employees and their employer subject to the GDPR.[57] Interestingly, in a new set of rules, China is attempting to facilitate transfers of employee personal information by exempting it if such data is necessary to perform human resource functions or to administer collective employee agreements, assuming processing practices comply with China labour law requirements.[58]

For other types of more sensitive data, like key-coded research data, similar compromises could perhaps also be considered assuming reasonable steps are taken to confirm that such data should not be deemed of interest to public authorities, which could very well be a reasonable assumption to make in several instances. Interestingly, China has recently attempted to soften its stance for data generated in international trade, academic cooperation, multinational manufacturing and marketing activities that do not contain personal information and important data.[59] It remains to be seen whether China will agree to find that individual-level personal data could be transformed into anonymised data without necessarily aggregating the data.

On the basis of the UK GDPR, the ICO has developed a transfer risk assessment tool that is based upon the classification of personal data in relation to risk levels.[60] It is clearly stated within the tool that when categories of personal information are associated with low-harm risks, it is possible to proceed with the transfer, no matter what the response might be to the next questions, which relate to human rights and enforceability risks. The ICO is thus trying to set forth a fine-grained approach to data transfers on the

---

however slightly different from P. Swire et al, as when defender techniques are user focused as opposed to application focused and consist in systematically profiling users to eventually impact upon their legal situations, there is an argument that the single source of truth should be located within a jurisdiction offering an adequate level of protection. From a design standpoint, it is in principle possible to abstract the audit layer of a technology stack and let the user choose its location.

[56] See Annex I, III Supplementary Principles, para. 9:(e)(i) "For occasional employment-related operational needs of the participating organization with respect to personal data transferred under the EU-U.S. DPF, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the participating organization has complied with the Notice and Choice Principles."

[57] 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 on 14 February 2023 ("the second criterion implies that the concept of "transfer of personal data to a third country or to an international organisation" only applies to disclosures of personal data where two different (separate) parties (each of them a controller, joint controller or processor) are involved.")

[58] See "Regulation and facilitation of cross-border flow of data" discussed in Y. Zhang, Personal Data Protection and Data Transfer Regulation in China, Chapter 3 of the compendium.

[59] Ibid.

[60] ICO, Transfer Risk Assessment Tool, n(46). The ICO explains that there are two ways to comply with chapter 5 of UK GDPR.

basis of the UK GDPR, which would suggest that there is no reason why the EDPB could not pursue a similar objective, as long as it is clear that it is the likelihood of human right violation that should be used to set the threshold as harm is not a prerequisite to the protection of human rights. With this said, the harm classification produced by the ICO raises questions. It is not clear, for example, why habits should be classified as low risk when these are the basis of intrusive profiling. Besides, one should look beyond the data and take into account the purpose of the data flows and the level of data-subject intervenability to strike a more legitimate compromise.

Another way to explain the reluctance of EU supervisory authorities to endorse a fine-grained approach could be found in the view that the Schrems II decision necessarily endorses a one-size-fits-all approach that makes it impossible to refine the profile of the attacker in the light of the circumstances of the case at hand. It is unclear whether the CJEU ever went that far, however.

In addition, a one-size-fits-all approach is hard to reconcile with a definition of restricted transfers that is also a compromise. The EDPB definition for example, which builds upon the CJEU case law,[61] excludes data flows between data subjects and entities acting as controllers or processors of personal data, thereby requiring an interaction between two types of covered entities.[62] The EU definition of data transfers is thus the fruit of a compromise between the will to ensure a high level of data protection and the acknowledgement of the realities of cross-border data exchanges enabled by the Internet. Since 2018, this compromise is reached with the implementation of a safety valve: Article 3(2) of the GDPR.[63] In other words, even if data flows departing from data subjects are not deemed restricted transfers within the meaning of Chapter V, it is very likely that the data importer will be subject to the GDPR anyway. There is no reason why such a safety valve should not be used for low-risk data or better low-risk processing activities between covered entities, as data flows between data subjects and covered entities could very well lead to situations of high risks for the fundamental rights and freedoms of individuals.

[61] See CJEU Case C-101/01 Bodil Lindqvist 6 November 2003 ECLI:EU:C:2003:596.

[62] This approach is peculiar to the EU as Convention 108+ adopts a different approach and defines restricted transfer as access by a recipient that is not a party to Convention 108+, making the role of the parties to the data flow irrelevant (see Article 14 read in the light of the Explanatory Report). The same approach has been adopted by China, but as mentioned above, this country is now considering loosening its approach. Of note, Brazil also seems to go down a similar path by distinguishing between data transfer and data collection and excluding the latter from the remit of transfer restrictions. See P. Trigo Kramcsák, Personal Data Protection and Data Transfer Regulation in Brazil, Chapter 1 of the compendium.

[63] This begs the question why not using this safety valve for all types of transfer in an attempt to simplify the regulatory burden. There are good reasons not to go in this direction though, in particular if the goal is to force data importers to shield themselves from local public authorities. In addition, Kuner makes it clear that ”data transfer rules also provide more enforcement possibilities than does extraterritorial application of the GDPR, since many transfer rules can also be enforced against the data exporter in the EU.” Chistopher Kuner, Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU’s Ambition of Borderless Data Protection, Paper no. 20/2021, April 2021, Legal Studies Research Paper Series, University of Cambridge, p. 25. Besides, he also observes that ”the appointment of a representative as a way to improve enforcement of the GDPR against non-EU parties has thus far proven largely toothless.” Ibid, p. 12.

What is more, an adequacy decision is always a compromise.[64] Take the example of New Zealand, which has received an adequacy decision prior to the GDPR, and of which validity has been confirmed post GDPR a few months ago by the European Commission.[65] Data originating from the EU could leave New-Zealand, on the basis of Principle 12 of the Privacy Act 2020,[66] without any restriction when the data importer is subject to the Act.

A compromise is also implicitly set forth when capabilities to access protected data from third countries (in the absence of actual data flows) are not considered sufficient to trigger the applicability of GDPR Chapter 5.[67]

Recommendation: Consider developing a fine-grained data transfer assessment method.

3.3. Data Transfers, Trustworthiness, and PETs

Despite recent references to trust,[68] governing CBDTs is fundamentally about forcing the production of trustworthiness evidence. Trust and trustworthiness are two different, even if related, concepts. While trust is an attitude, trustworthiness is a property.[69] Said otherwise, trust is a leap-faith on which to base a

[64] One compromise that has often been criticised is the adequacy decision issued in favour of Japan, despite clear evidence that the level of enforcement was rather weak. The same is true with the adequacy decision issued in favour of Israel that has been recently confirmed following the review process of 11 pre-GDPR adequacy decisions.
[65] Report from the Commission to the European Parliament and the on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM(2024) 7 final, 15 January 2024.
[66] Privacy Act 2020, Section 22, Information Privacy Principle 12(1)(b).
[67] See e.g., EDPS, Decision on the CJEU's use of Cisco Webex video and conferencing tools, 13 July 2023, available at https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/2023-07-13-edps-cjeus-use-cisco-webex-video-and-conferencing-tools_en#:~:text=In%20its%20Decision%20published%20on,%2C%20bodies%2C%20offices%20and%20agencies, accessed 28.01.24, para. 35 ("The EDPS considers that transfers resulting from unauthorised access by third country entities, which are merely potential and in no way foreseeable in light of the content or purpose of a contract or another stable relationship between the parties, do not fall under the scope of Chapter V of the Regulation"). There does not seem to be perfect consensus on the matter, however.
[68] See the Data Free Flow with Trust initiative promoted at the Group 7 (G7) and Organisation for Economic Co-operation and Development (OECD) levels. See e.g., Japan Digital Agency, Data Free Flow with Trust, available at https://www.digital.go.jp/en/dfft-en, accessed 28.01.24; OECD, Moving forward on data free flow with trust: New evidence and analysis of business experiences, OECD Digital Economy Paper, n°353, available at https://www.oecd.org/sti/moving-forward-on-data-free-flow-with-trust-1afab147-en.htm, accessed 28.01.24.
[69] There are many conceptualisations of trust stemming from different disciplines, including economics, sociology, psychology and law. The trustor's willingness to be vulnerable is central to most conceptions of trust. On the other hand, when trustworthiness is distinguished from trust, it is usually described as a property of the trustee that can ground a trustor's expectations, when trust is conceived as the expression of a rational choice (i.e., cognitive trust as opposed to affective trust). Trust and trustworthiness are, however, often wrongly conflated with each other. See e.g., M. Greenwood & H. Buren, Trust and Stakeholder Theory: Trustworthiness in the Organisation-Stakeholder Relationship, 95 (2010), 425-438; H. Sekhon, C. Ennew, C., H. Kharouf, & J. Devlin, Trustworthiness and trust:

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. The starting point in the context of a commercial relationship is trustworthiness. A party to a commercial relationship relinquishing control over governed data should thus require from the other party or other authoritative sources evidence of trustworthiness.

Trustworthiness in a CBDT context can be established at two levels: at the jurisdictional level and/or at the entity level. As a result, two types of trustworthiness evidence are distinguished. When the evidence focuses upon the regulatory framework of the jurisdiction in which the data importer operates, it relates to *institutional trustworthiness*, while when it focuses upon the commitments and/or behaviour of the data importer itself, it relates to *relational trustworthiness*.

CBDT tools are thus a means to produce evidence of trustworthiness: either institutional trustworthiness, e.g., with adequacy decisions, or relational trustworthiness, e.g., through SCCs, BCRs or certification.

Importantly, even when CETs are implemented to mitigate against the absence of institutional trustworthiness, which is problematic when Restriction Pattern #2 is applicable, evidence of relational trustworthiness is still relevant. It often makes sense to subject data importers to contractual obligations to make sure appropriate context controls are put in place, e.g., obligation to implement strict access control, to comply with purpose limitation, or not to collude with other data sharing scheme participants. If a claim of legal anonymisation is asserted, context controls remain relevant even when the strongest CETs are implemented (e.g., through global differentially private methods) and enforcement assurances should be sought through appropriate CBDT tools.

What is more, when a CET setting aims to preserve some level of data subject intervenability, which should be facilitated by a query setting, it may make sense to impose upon data importers an obligation to assist the data exporter when responding to data subject requests.

What this shows is that data transfer tools such as SCCs, BCRs or certification, of which primary purpose is to evidence relational trustworthiness, will still be needed and CETs should only be conceived as complements to such tools.

Recommendation: Consider closely intertwining PETs and a CBDT tools workstreams.

4. Conclusion

Incentivising the free flow of data through PET promotion requires carefully thought-through nuances. First, such an effort implies creating a consensus upon a fine-grained approach to data transfer, which on

influences and implications, Journal of Marketing Management, 30(3-4) (2014), 409-430. See also references listed in S. Stalla-Bourdillon, Relational Trustworthiness for Cross-Border Data Flows: on Certification and Model Clauses, Chapter 5 of the compendium, section 2.1.

occasions has been welcomed with suspicion by regulators as it is challenging to draw distinctions between processing activities on the basis of individual impact. Second, it requires formalising a contextual risk-assessment method to help assess the legitimacy of the trade-off reached between two competing goals, utility and confidentiality. This method should comprise at least two steps:

1. A relatively narrower step during which the types of inferences addressed by the CET setting are explicitly identified and mapped against relevant controls

2. A broader step during which other data protection goals than confidentiality is taken into account, such as purpose limitation, fairness and data subject/end user intervenability.

Third, it requires acknowledging the ongoing relevance of CBDT tools. This is because in many instances claims of legal anonymisation should be made dependent upon downstream controls set by the data importer. Conceiving CBDT tools and PETs as alternatives is thus inherently flawed.

This paper includes five recommendations for policymakers interested in setting or contributing to PET workstreams and who are engaged in actions to address the fragmentation of data flow regimes at the global level.

Key Recommendations:

1. Consider producing a list of recommended PET use cases starting with use cases that are in the public interest considering a wide range of dimensions of concern
2. Consider producing guidance on threat modelling techniques
3. Consider showcasing CET settings that are able to preserve data-subject and end-user intervenability
4. Consider developing a fine-grained data transfer assessment method
5. Consider closely intertwining PETs and a CBDT tools workstreams

Key Recommendations:

The paper has shown that CETs on their own are implemented to pursue very limited objectives. In addition, it has made clear that while some of these CETs are very powerful in the light of the particular objective they aim to pursue, they always imply a trade-off, i.e., a decision to prioritise utility over confidentiality. Therefore, this paper suggests that CET selection and implementation should be use-case specific and take into account a wide range of dimensions of concern, including the legitimacy of processing purposes, fairness, the level of data-subject or end-user intervenability, as well as eventual broader implications, such as implications in terms of data and infrastructure monopoly.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE OF CROSS-BORDER DATA FLOWS

RELATIONAL TRUSTWORTHINESS FOR CROSS-BORDER DATA FLOWS: ON CERTIFICATION AND MODEL CLAUSES

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

Executive Summary

While top-down harmonisation 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 endeavour 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]

---

[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.

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.

While top-down harmonisation 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 endeavour beyond a small

[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.
[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

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 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.[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

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.

[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.

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 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

[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-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.

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 behaviour of the data importer vis-à-vis the data exporter.[19] A one-

[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 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."

off relational 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

[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.

production of such pieces of evidence.[22] One way to help reduce such inconsistencies would be to adopt a holistic approach to the 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

[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-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

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.

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 behaviour has been monitored to generate the data, or the data

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.
[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.

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 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

[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).

[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.

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]

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.

[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).

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

[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.

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 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

[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.

chance to 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]

---

[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.

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.

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

[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.

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 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,

---

[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.

[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.

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]

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

---

[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 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

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

---

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.

certifications and SCCs. It 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

[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.

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.

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

[75] https://www.iso.org/standard/71670.html, accessed 1.5.24.
[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.

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 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

---

[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.

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

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.

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

[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.

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 to export privacy and data protection standards could be considered as de facto higher

[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.)

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.

The European Union's 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

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

[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.

[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

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.

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 Model Contractual Clauses (MCCs)

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

---

[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.

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]

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

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

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 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

[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".

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

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]

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

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

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

[129] See all references mentioned in n(85).

	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 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

[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

decentralized architecture for managing (analytical) data at scale. It enables the decomposition of an organisation'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 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

---

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.

[139] The least privilege principle is the security version of the minimisation principle and is now appearing in

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

---

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.

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 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

[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.

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, 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.

4.1. 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

[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.

[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.

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 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

[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.

for achieving higher levels of assurance in CBDTs.

4.2. 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 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

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

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 harmonisation 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.

4.3. Free Trade and 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

[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

limited exceptions for "legitimate public policy objectives".[156] Additional provisions were discussed, such as the EU's proposal for an exception 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 trust marks 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

---

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).

[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.

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 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

[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.

[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).

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 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

[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.

[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.")

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.

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 harmonisation 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.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank