OECD publishing

MOVING FORWARD ON DATA FREE FLOW WITH TRUST

NEW EVIDENCE AND ANALYSIS OF BUSINESS EXPERIENCES

OECD DIGITAL ECONOMY PAPERS
April 2023 **No. 353**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report, *Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences*, was prepared by the Working Party on Data Governance and Privacy (WPDGP). It is based on the responses to a survey about businesses' perspectives on the importance of cross-border data flows and trust, and related compliance challenges as more laws and regulations applicable to data flows are adopted globally.

Francesca Casalini and Shihori Maeda drafted this report under the guidance of Clarisse Girot from the OECD Secretariat. Steve Wood, Director and Founder of PrivacyX Consulting, former United Kingdom Deputy Information Commissioner and former Chair of the WPDGP, has contributed to this work as an external consultant.

This report was approved and declassified by written procedure by the Committee on Digital Economy Policy (CDEP) on 24/04/2023. It was prepared for publication by the OECD Secretariat.

The authors gratefully acknowledge the discussions with and key insights from private sector stakeholders listed in Annex A who have made this report possible. The authors also thank CDEP and WPDGP members for their helpful and constructive comments and discussions in developing this report.

This publication contributes to Intermediate Output Result (IOR) 5.1 "Cross-border data flows with trust and data localisation" of the 2023-24 Programme of Work of the CDEP. It has been supported by a voluntary contribution from the Government of Japan.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/DGP(2022)13/FINAL

Table of contents

Figures

Executive summary

This report is based on a series of structured discussions with a sample of businesses and legal practitioners (hereafter "businesses") that conveyed challenges and opportunities on 'data free flow with trust' (DFFT) from a business-centric perspective. As such, the report's aim is limited to informing policy discussions on DFFT, without prejudice to each country's regulatory autonomy to adopt any approach that might best reflect its legitimate policy objectives and regulatory preferences.

Moving forward on DFFT: An analysis of business experiences

Cross-border data flows are critical for the global economy and achieving the United Nations Sustainable Development Goals. As repeatedly affirmed by policy makers in recent years, DFFT is a policy priority in the 21st century. While a comprehensive definition of DFFT is difficult to formulate, the protection of privacy and data protection across borders have been identified as critical aspects of the DFFT agenda, along with security and intellectual property rights protection, among others.

The voices of many and different stakeholders are thus needed to inform DFFT discussions. This report starts by providing a mapping of business views regarding compliance with privacy and data protection requirements for cross-border data flows. Additional work reflecting other stakeholders' perspectives on these and other relevant issues could complement this work in the future.

Themes from the discussions with business on cross-border flows of personal data

Businesses indicate that they attach fundamental importance to the protection of personal data and privacy, for the protection of the rights of individuals, of sensitive business data, and as an economic asset and competitive advantage. At the same time, they also highlight that while privacy and data protection frameworks aimed at generating trust and facilitating data flows build on commonalities and elements of convergence, challenges remain on how to fully "operationalise" them globally to ease compliance and facilitate cross-border data flows.

Businesses suggest that, from their perspective, greater transparency, predictability and cross-sectoral consistency in transfer requirements would facilitate more effective compliance strategies and protection for individuals. They indicate that adequate protection of personal data, including the rights of individuals regarding that data, requires long-term investment in accountability, training and risk management programmes. In this sense, they indicate that the current complexity of analysing and implementing compliance can divert their own limited resources from those needs. Businesses also highlight the importance of ensuring that regulations remain attuned to developments in how data flow within the global economy as technologies such as artificial intelligence (AI) and cloud computing rise in use.

In this context, businesses indicate a greater need for:

- a set of cohesive principles and rules for cross-border transfers of personal data and associated means to ensure safeguards are implemented to realise effective data protection globally

- policies, regulations and regulatory interpretations that provide a practical balance between certainty and flexibility and focus on effective protection (rather than mere formal compliance) to build trust
- solutions that match business realities and support companies' data governance strategies broadly
- more inclusive dialogue to achieve a shared understanding of technological developments and how they can support privacy in the context of DFFT.

Against this background, businesses note that existing mechanisms for data transfers (such as rules on accountability, adequacy findings, binding corporate rules, contracts, certifications or consent) have features and characteristics that could be further leveraged to improve compliance processes and support more effective data protection. While each transfer mechanism has both strengths and limitations, businesses suggest that some are more mature than others. They indicate that the low uptake of some of them today is not necessarily indicative of limited potential but could be due to the time needed for consolidating them into a business case, the entry burden or the challenging approval process. Costs were especially noted by legal counsels as a challenge for small and medium-sized enterprises (SMEs).

The businesses consulted indicate that legal solutions could aim to better accommodate evolving business priorities. They consider that mechanisms and legal bases for data transfers will be most impactful when they ensure protection of fundamental privacy rights, effective privacy accountability and when they can be leveraged with internal privacy management programmes and compliance structures. Businesses welcome the current impetus to develop scalable solutions at the regional and global level particularly with respect to some transfer mechanisms. They encourage the continuation of efforts by governments and regulators to advance solutions that can bridge different regulatory systems.

Key findings

Moving forward on DFFT requires an integrated policy approach, both domestically and internationally, to build trust. The capacities of governments and regulators, including privacy but also sectoral regulators, to co-operate across silos, borders and at different levels simultaneously are key to supporting organisations in their efforts to build trust and multi-jurisdictional compliance. Overall feedback suggests that the impact of cross-border data flows on other policy objectives depends both on a variety of domestic policy settings and the nature and degree of international regulatory co-operation on data and data flows.

Based on these business consultations, advancing the DFFT agenda with respect to data protection and privacy could be further facilitated by:

- **Enhanced dialogue**: Providing businesses and policy makers with DFFT-related information. This could cover business experiences, policy and regulatory development, use cases, good practices and examples of solutions, including technological solutions, in place in the business community.
- **Greater legal certainty**: Building trust through domestic policies that are transparent, consistent across sectors, and focused on outcomes – meaning aimed at providing effective protection to individuals, instead of cases where formalities-focused compliance solutions do not necessarily contribute to effective data protection.
- **Further incentives for a culture of global compliance and trustworthiness among business**: Fostering and incentivising a global privacy and data protection culture for companies built on shared principles, compliance, organisational accountability, streamlined processes and a strong business case for a range of complementary transfer mechanisms.
- **International regulatory co-operation on privacy and data protection**: Building a coherent global regulatory landscape leveraging the full range of options for international regulatory co-operation to ensure a high standard of data protection and uphold trust around privacy and data protection globally. Such efforts should build on multistakeholder experience across different disciplines, sectors and levels of government and a common framework to address these issues holistically.

1 Introduction: A business contribution to help move forward on DFFT

1.1. The complexity of defining the next steps for advancing DFFT

Today's global economy is founded on data flowing domestically and across borders, and the challenges and the repercussions of data access and sharing across the world are an increasingly debated topic in policy circles (OECD, 2022[1]), in the media, in civil society and among the public.

Policy discussions about cross-border data flows are complex because they touch on diverse and legitimate policy concerns – protecting privacy and personal or other sensitive data, proprietary information and intellectual property rights, digital security and safety, national and public security; ensuring trusted regulatory access to data; facilitating international trade and development, supporting supply chains, innovation and growth, and promoting fair competition (OECD, 2022[2]).

Discussions are also complex because data are ubiquitous, non-homogenous and relevant across multiple disciplines. Stakeholders involved come from different regions, policy communities and backgrounds; they operate in different settings based on different references, presumptions, and assumptions; and they have different priorities and use different terminologies. Combined with varying levels of understanding about the implications of the global use of digital technologies, such as cloud computing and AI, these differences can result in gaps in knowledge and misunderstandings.

In addition, broad and deep-seated distrust towards business models involving personal data and large digital incumbents (Chevalier, 2022[3]), and a perception of regulatory capture by those incumbents, contributes to a level of mistrust around cross-border data flows, in particular with respect to privacy. Stakeholders suggest that this mistrust might sometimes obscure the benefits of cross-border flows for other sectors and actors.

Finally, previous work has highlighted the need for continued co-operation based on commonalities, complementarities and elements of convergence in the regulation of data and cross-border data flows around the world (OECD, 2022[2]; 2022[1]; Robinson, Kizawa and Ronchi, 2021[4]; Casalini, López González and Nemoto, 2021[5]; Casalini and López González, 2019[6]) to advance DFFT (OECD, 2022[2]; Digital Agency, Japan, 2022[7]).Nevertheless, while mechanisms are being developed to bridge different regulatory systems, some challenges remain at the compliance level for businesses to "operationalise" such commonalities in their daily transfer and compliance processes, but the reasons for such challenges have not been the object of thorough study.

1.2. Report's focus: challenges at the compliance level for cross-border transfer of personal data, as reported by businesses and legal counsels

Given the diversity of issues to be addressed to advance DFFT, there cannot be any silver bullet solution. The DFFT vision can only be built over time as all relevant subjects and perspectives for developing trust in data flows emerge and more stakeholders get involved.

This report reflects responses to a survey aiming to contribute to the broad objective of moving forward on DFFT, focusing on compliance with privacy and data protection requirements for cross-border transfers from the perspective of businesses. Through extensive consultation with a diverse set of companies and legal practitioners around the world,[1] this exercise aims to map challenges faced by businesses and provide some initial insights on ways forward to better "operationalise" the commonalities, complementarities and elements of convergence that countries share in their data protection frameworks.

Contributing to the multi-faceted policy discussion on DFFT through this approach provides only a partial perspective. A few clarifications must be made regarding the scope of the exercise:

- Despite DFFT often being treated as a single policy issue, building trust around cross-border data flows requires addressing multiple issues. Specific work is ongoing at the OECD on several of the other themes that contribute to the broad DFFT agenda, including on data localisation (López González, Casalini and Porras, 2022[8]; Svantesson, 2020[9]); cross-border co-operation in the enforcement of data protection and privacy laws (OECD, forthcoming[10]); government access to personal data held by the private sector (OECD, 2022[11]); enhancing access to and sharing of data (OECD, 2019[12]; OECD, 2021[13]); privacy-enhancing technologies (PETs) (OECD, 2023[14]); and metrics and measurement.
- The discussions with businesses that informed this report focused on privacy and personal data. However, sectoral and other frameworks also impact business compliance processes. For instance, equally relevant in DFFT discussions regarding personal data are domestic and international frameworks in the fields of trade, telecommunications, intellectual property (including World Trade Organization agreements) and national security, as well as emerging frameworks addressing "non-personal data". In 2022, Group of Seven (G7) members committed "to better understand the opportunities and challenges created by cross-border data flows. This includes deepening our understanding of existing regulatory approaches and instruments enabling DFFT, including related to privacy, data protection, security, and the protection of intellectual property rights" (Federal Ministry for Digital and Transport, 2022[15]).
- Compliance challenges also exist in the public sector. Today data are increasingly shared across borders between public and private actors, for regulatory co-operation, for the achievement of other public policy objectives, or for the use of private sector solutions by the public sector. It would thus be useful to consult public sector actors as well in the future to complement the findings of this report.
- This report only focuses on the views of businesses and legal practitioners on the topic of privacy and personal data. It does not reflect the views of non-business actors such as civil society groups and consumer associations, and of regulators and policy makers, whose views are also essential to understand the rationale of current compliance requirements, although some of them provided comments and inputs into the draft. As such, the report's aim is limited to informing policy discussions by providing an overview of business perspectives regarding DFFT, without prejudice to each country's regulatory autonomy to adopt any policy and regulatory approaches that might best reflect its legitimate policy objectives and regulatory preferences. Additional work reflecting other stakeholders' perspectives on these and other relevant issues could complement this work in the future.

1.3. Five themes from the discussions with businesses, leading to the structure of the report

The messages that emerged from the discussions with business and legal counsels can be summarised along five common themes, which provide the structure of the report:

- Businesses express a growing need for cross-border data flows (Section 2).
- The data protection and privacy landscape is evolving quickly (Section 3).
- Businesses express concern in relation to growing compliance challenges globally (Section 4).
- Companies want to be empowered to carry out responsible cross-border data flows and meaningful data protection (Section 5).
- Existing legal bases and mechanisms for cross-border data flows could be further leveraged to advance DFFT (Section 6).

The report concludes with takeaways that derive from these discussions (Section 7), noting the limitations as outlined above.

2 Businesses express a growing need for cross-border data flows

As digital technologies become increasingly pervasive, cross-border flows of data underpin business operations in all industries and geographical regions (UNCTAD, 2021[16]). While the exact contribution of cross-border flows of data to global value chains remains elusive, as it cannot be easily discerned from either trade or information and communications technology (ICT) statistics, it is commonly acknowledged as being extremely significant and even vital for the global economy. Businesses consistently point to the critical nature of cross-border flows of data, including personal[2] and other data types, not only in high-tech ICT sectors but across many, if not all, economic sectors, such as agriculture, life sciences, manufacturing, retail, aviation and finance (Global Data Alliance, 2022[17]).

It is impossible to exhaustively list the many types of data transfers that enable the daily operations of companies. However, cross-border data transfers are generally reported to fall into two main buckets.

First, organisations transfer data for the purpose of efficiency, to connect and scale their internal business processes. Efficiency gains pertain to a wide range of purposes, such as improved digital security and centralised management of key business functions. Some companies even transfer data as an intrinsic part of their business models to serve customers in different regions around the world and to join up analytics to create value from global datasets. In practice, companies report that they often think of their data-processing activities as a single global processing operation organised by business units and not by legal entities, regardless of the multiple countries across which the data are collected and processed.

"Internal operations" are now often also external, through the integration of third-party-provided capabilities, such as employee expense management capabilities, booking engines, and overall cloud computing services, among others. Today many organisations, including SMEs, depend upon a cross-border ecosystem of multiple parties to run internal functions and to conduct an organisation's business.

Second, companies commonly share data across borders for necessity, to engage with external stakeholders that need access to data, or for compliance with other regulatory requirements. Examples include health data transferred to other organisations for research, such as collaborative vaccine research; financial data transferred to overseas investors pursuant to an asset sale agreement or to carry out know-your-customer checks; or passenger data to manage international travel.

Overall, businesses are becoming more closely linked to long and complex digital supply chains, with multiple data transfer relationships to map and understand for data protection compliance purposes and for which they need to make rapid and regular decisions, day by day, week by week.

In this context, businesses report unanimously a fast-increasing number of regulatory requirements for cross-border transfers of personal data in all regions of the world and economic sectors. They note a growing challenge in balancing the structural need of transferring data with the regulatory risk they face due to the range of transfer rules they must respect in order to ensure compliance with legal requirements but that they may not be capable of fully complying with at once.

3 The data protection and privacy landscape is evolving quickly

3.1. Data protection laws are becoming ubiquitous at the global level

As of 2021, 71% of countries had data protection laws in force, 9% had draft legislation, and 15% had no legislation (UNCTAD, 2021[18]),[3] with developments continuously taking place in this space (Greenleaf, 2023[19]). Most of these data protection and privacy laws have extraterritorial application so that they can apply cumulatively to the same processing activities, and virtually all of them contain provisions on cross-border data transfers (Casalini and López González, 2019[6]). While this trend is regarded as an undeniably positive signal of increased attention to privacy and data protection issues, it also represents a fast-evolving range of somewhat diverse compliance obligations that businesses must comply with.

Some key developments in the data protection and privacy landscape over the period 2021-23 alone help to illustrate the rapidly changing regulatory environment in which companies operate, particularly with regard to cross-border data transfer requirements:

- Alongside the progress of negotiations between the **European Union** and the United States to replace the Privacy Shield adequacy decision, the European Data Protection Board (EDPB) has issued many guidance documents that clarify or implement the provisions of Chapter 5 of the GDPR. The European Commission has adopted further adequacy decisions (including the EU-Japan mutual adequacy arrangement) and a major modernisation of standard contractual clauses. In parallel, the Digital Services Act and Digital Markets Act entered into force in November 2022, following the Data Governance Act in June 2022. The proposed EU Data Act, which aims at regulating cross-border sharing of non-personal data through provisions modelled after those of GDPR, is also making progress.
- The **United Kingdom** is charting its own course post-Brexit, replacing the system based on EU GDPR while also seeking to retain EU adequacy. The government appointed an Expert Panel on Data Flows that is due to publish a report with recommendations later in 2023. The United Kingdom is reportedly pursuing an agile, risk-based and multilateral-oriented approach.
- In the **United States**, calls for federal privacy and data protection legislation have increased, leading to the House Energy and Commerce Committee approving the American Data Privacy and Protection Act in July 2022, although its future in the new Congress is uncertain. Several state privacy laws have taken effect in 2023, including the California Privacy Rights Act. In August 2022, the Federal Trade Commission (FTC) filed an Advanced Notice of Proposed Rulemaking to explore rules to "crackdown on harmful commercial surveillance and lax data security", seeking comments on "harms stemming from commercial surveillance and whether new rules are needed to protect people's privacy and information" in areas including algorithms, ad delivery, demographic data, engagement and the ecosystem's effects on kids and teens. Any change to US legislation or FTC rules would impact a majority of digital activities across the globe that rely on US providers.

- Several changes have occurred in other key countries of the common law world. In March 2023, the House of Commons of **Canada** announced plans to resume the debate on the proposed Bill C-27, Digital Charter Implementation Act, 2022, at second reading. The omnibus bill contains proposals for the Consumer Privacy Protection Act, Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act. In February 2023, the **Australian** Attorney-General's Department of Australia released its highly anticipated review of the Privacy Act 1988, a significant step in the reform of the nation's privacy law, which also impacts the overseas disclosure of personal information.
- **Brazil** passed the General Data Protection Law in 2019, a “high water mark” law that contains international transfer provisions loosely inspired by the GDPR, including by reference to legal bases for transfers, such as adequacy and standard contractual clauses. Comparable data protection regimes evolving from the legal doctrine of “habeas data”, which is found in practically all Latin American constitutions, exist or are being developed in countries such as **Argentina**, **Colombia**, **Costa Rica**, **Mexico**, **Peru** and **Uruguay**. The Ibero-American Network for Data Protection also issued guidance on transfers and standard clauses in October 2022.
- In 2020, some broad changes were made to the **Japan** Act on Protection of Personal Information (APPI), which took effect in 2022. These amendments were made as part of a policy to review the APPI every three years. In addition to expanding some individuals’ rights and companies’ obligations, including in relation to providing information to individuals about cross-border data transfers, these changes sanction the extraterritorial application of the law. They empower the Personal Information Protection Commission to make requests to foreign entities about the processing of data and issue orders for violations of the APPI.
- In 2023, **Korea** also made broad amendments to the Personal Information Protection Act. While the changes generally facilitate cross-border transfers of data by broadening the possible condition for executing them (consent was previously the only option in some cases), the changes also expand the application and reinforce the penalties of these requirements. It remains to be seen how some of these new conditions will be enforced by the regulator in practice.
- Several changes also occurred in Southeast Asia. **Singapore**’s Personal Data Protection Act was amended in 2021, introducing the concepts of legitimate interests and business improvement as exceptions to consent and reinforcing the powers of the Personal Data Protection Commission, among others. The Personal Data Protection Act of **Thailand**, initially signed in 2019, fully entered into force on 1 June 2022 after being postponed due to the pandemic. In October 2022, the Personal Data Protection Bill of **Indonesia** turned into law after many years of uncertainty. Both laws include GDPR-style data transfer provisions. The Personal Data Protection Decree developed by the Ministry of Public Security of **Viet Nam**, in draft form since early 2021, should be released in 2023 and remove state approval prior to the transfer and storage of original data in Viet Nam, but subject to a transfer impact assessment, a data transfer agreement, and a post-transfer report to the personal data protection authority.
- In the **People’s Republic of China** (hereafter, “China”), the Personal Information Protection Law requires companies to conduct security assessments before transferring personal data and important data abroad. In 2023, the Cybersecurity Administration of China published guidelines concerning security assessments and its own standard contract for transfers. More recently, new draft certification requirements for cross-border transfers were submitted for public consultation. However, it remains unclear how the different pieces of the legal puzzle will be applied in practice, how it will work with other key legal frameworks, or how far localisation of data will be required by the regulators. The announcement on 7 March 2023 of the creation of a new National Data Bureau to regulate data-related issues (including data exports) and centralise data management and enforcement also adds to the complexity.

- In late 2022, the Government of **India** announced the close adoption of the Digital Personal Data Protection Act, 2022, the third version of the much-awaited data privacy law of the country. The previous iteration of the bill (withdrawn in October 2022) intertwined strict localisation requirements with more "traditional" accountability-based data transfer provisions. Following stakeholder feedback, a new draft of the bill was published in November 2022, but in March 2023, the government released a radically new version of the previous provision on cross-border data flows which could include an "allowed-by-default model".
- Many countries in the Middle East have recently adopted data protection laws, such as **Qatar** (2016), **Bahrain** (2019), the **United Arab Emirates** (2021) and **Saudi Arabia** (2021). While drawing on the GDPR and other international models, the laws vary from those and between them and contain provisions on data localisation and regulatory authorisation procedures broadly motivated by national interest and security concerns. In 2021, the Ministry of Justice of **Israel** announced proposals to update its data protection laws to improve the regulatory scope, key definitions and increase the enforcement powers of the Privacy Protection Authority.
- Despite attempts such as the 2014 Malabo Convention or the 2022 African Union Data Policy Framework, African countries have been taking different paths with respect to privacy and personal data protection regulation. Where laws exist, there are significant differences in rules and no consistent mechanism for cross-border data flows. **South Africa**, **Botswana** and other countries have been adopting regulation that permits the transfer of data subject to certain conditions, although there are still concerns over the effective implementation of some of these measures and transparency issues on how adequacy decisions are made. Some other countries, such as **Nigeria**, **Rwanda** and **Zambia**, have also recently adopted laws with elements of data localisation, reflecting a focus on the concept of "data sovereignty". While the enforcement of these regulations remains unclear, several concerns exist due to the unstable power infrastructure that sustains data centres in these countries.

The impact of these regulatory developments is more or less significant depending on the organisations' geographical footprint. All, on the other hand, point in the same direction of granting extraterritorial effect to the law (noting that there appears to be some confusion as to the intersection of extraterritorial application and transfer rules), extended rights for individuals, reinforced powers for regulators, and provisions relating to cross-border transfers, which must be combined with sectoral legislation as well.

3.2. Increased regulatory co-operation means better privacy protection globally but also increased regulatory risks

As more data protection laws are adopted, more data protection authorities are established, with variable periods between the adoption of a law and the effective establishment of an enforcement authority. More regional and global regulatory networks are also developing, and the enforcement powers and the capacities of data protection regulators to co-operate across borders are being reinforced (Global Privacy Assembly, 2022[20]).

Across all regions, legal advisers consider that newly established regulators who had so far steered clear of costly enforcement actions that put them at risk of litigation, favouring instead the publication of advice, guidance and education material, have become more active in recent years, following perceived public demand and need for regulatory action. Enforcement action can include suspension of activities and fines, and criminal sanctions for business managers.

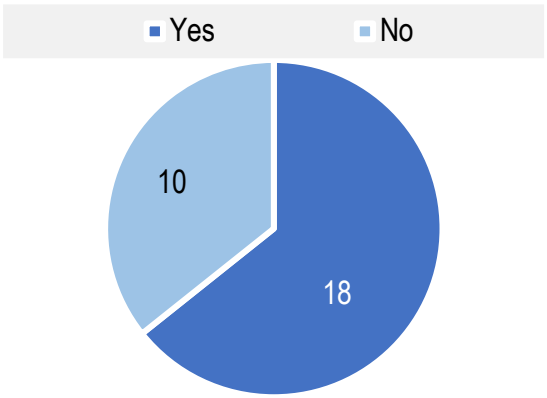
Authorities also increasingly co-operate on enforcement actions across jurisdictions. In 2021, more than half of the privacy enforcement authorities (PEAs) responding to an OECD survey said that they had faced situations where violations of privacy laws spanned two or more jurisdictions (OECD, forthcoming[10]). In a

notable example, the Clearview AI case led to the co-ordinated issuance of fines and enforcement orders in five European countries in 2022.

In this context, the OECD is also reviewing its 2007 Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.

Figure 1. Share of violations of privacy laws spanning two or more jurisdictions

Over half of respondent PEAs have faced situations where violations of privacy laws have spanned two or more jurisdictions



Source: OECD (forthcoming[10]), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Privacy Laws*.

4 Businesses express concern in relation to growing compliance challenges globally

Businesses and legal counsels unequivocally consider the steady growth of data privacy laws adopted and adapted around the world throughout the last decade as a positive development. Privacy and data protection legal counsels confirm that, over the years, companies have become more aware of data protection issues and devote more resources to data security and privacy.[4]

Companies all around the world face an increasing imperative of managing high expectations from regulatory authorities, individuals and business counterparts with respect to their data protection and data governance practices, particularly in cross-border contexts. Beyond protecting individuals' privacy and rights, businesses consider that the protection of personal data makes good business sense – it stimulates improved data management at large, is part of employees' expectations, and contributes to enhancing brand reputation. Consistent feedback is that data management is becoming more important as a factor in whether stakeholders will regard a business as trustworthy, and possibly provide an economic return.

Companies further acknowledge the operational, reputational and financial risks attached to data breaches and non-compliance with privacy and data protection rules. These expectations are particularly high concerning compliance with the GDPR, which remains a reference also for companies not operating in the European Union, although more recent legislation in other key jurisdictions is also increasingly drawing companies' attention.

At the same time, companies suggest that the current regulatory landscape presents some challenges at the compliance level. While a level of complexity is intrinsic to any regulated environment, better investigating the sources of difficulty reported by companies in their compliance processes is helpful to identify the policy and legal responses that might be needed – in line with good regulatory practices to deliver better regulatory outcomes (OECD, 2020[21]).

While welcoming the increasing cooperation within and between certain networks of privacy regulators, businesses identify some compliance challenges impacting their activities in the areas of cross-border transfers of personal data: legal uncertainty; difficulties in elaborating regional or global compliance strategies; and a risk of compliance fatigue.

4.1. Legal uncertainty

Businesses suggest that an important challenge to compliance activities today is the lack of legal certainty in a growing number of jurisdictions. While they note that the trend towards commonalities and elements of convergence across privacy and data protection frameworks around the world carries with it a promise of reducing legal uncertainty in the long term, they also note that it is not sufficient as such for them to streamline compliance processes under multiple national and sub-national rules. Conversely, they indicate that the reduction of legal uncertainty is a decisive factor in reaping the benefits of such commonalities and

elements of convergence in practice. In this regard, companies chiefly indicate a need for greater transparency and cross-sectoral consistency in transfer requirements.

4.1.1. Transparency

As a first matter, companies and counsels indicate a need for transparency at the law and policy levels. They consider that the legislative process should be multi-stakeholder and result in text that is accessible and clear to increase buy-in and facilitate compliance. An example relates to ambiguities in the definition of "data transfer to a third country" in some laws or to the lack of a clear distinction in the law between data controllers and processors, which makes the allocation of responsibilities challenging.

More broadly, language and translation issues are also highlighted as critical in ensuring transparency and certainty when operating across borders. Companies often must anticipate the adoption of new laws without a reliable translation of the draft text, and they sometimes are not certain that they have the correct version of it in the first place.

Uncertainty about the application of data transfer rules or their lack of flexibility in practice may also create frictions that hinder data from being transferred altogether, even when this outcome is far removed from the lawmaker's original intention. For instance, requirements to obtain individuals' consent for personal data transfers in some jurisdictions may hinder transfers if no alternatives to protect individuals' rights are envisaged. In such cases, companies must either keep the data on shore to cater for the possibility that data subjects object or withdraw their consent or expose themselves to the risk of non-compliance.

Transparency is also fundamental in the context of any new law that is adopted, creating a period of uncertainty as to its effective application and discrepancy with previously accepted practices. In that vein, businesses also report instances where the institutional set-up needed to implement the regulation, chiefly a data protection authority, remains incomplete for up to several years after the entry into force of the law. It can indeed take time to establish a regulator, secure a budget and appoint members. Shortage of staff and time needed to set priorities can result in delays in issuing and implementing regulations and regulatory guidance, among others.

Against this background, businesses welcome the growing trend of complementing legal provisions with complementary documents, such as general application guidelines, sector-specific guidelines, or frequently asked questions (FAQs) to complement legal texts and clarify compliance expectations. Several companies also mention the importance of creating the conditions for permanent public-private co-operation to identify the unintended effects of draft regulations early and to develop alternative solutions.

4.1.2. Cross-sectoral consistency

Businesses report that a form of legal uncertainty also derives from a range of sectoral regulations, in addition to personal data protection frameworks, that create scenarios of overlap, if not displacement, of personal data protection frameworks. Data protection and compliance officers cite the growing number of intersections of personal data protection frameworks with other laws and regulations as compounding the difficulties mentioned above. This is especially the case when data transfers become subject to several sector-specific or data-specific rules that can clash with each other, as seen, for instance, in the interplay between the financial sector and personal data rules (IRSG, 2022[22]).

Another legitimate and rapidly growing concern is the emerging issue of protection of critical national infrastructure, which manifests itself in various privacy-impacting ways. These include expansion in 5G/Internet of Things (IoT)-device-level data capture and sharing and the increasing need for verification of identity and/or attribute (i.e. not a child), and for increased data sharing between organisations to facilitate detection and blocking of fraudulent activity. As a result, businesses also express a concern that in some jurisdictions data protection laws are increasingly overridden by new statutes addressing the

protection of critical national infrastructure – which they perceive to be even less harmonised than data protection statutes and to be enforced by authorities who have been less open to co-operation and approachable than privacy authorities, so far.

Companies struggle to deal with the cumulation of different sectoral requirements that require seeking information across multiple sources and engaging with multiple regulatory entities. Such engagement can prove challenging as sectoral regulators are often not familiar with the application of general personal data protection law, and vice versa, with risks of regulatory inconsistency attached. Companies and counsels suggest that greater inter-sectoral regulatory co-operation and one-stop-shop portals for keeping track of developments around transfers of both personal and other types of data in different jurisdictions would be a significant improvement to support compliance.

4.2. Businesses experience difficulties in elaborating regional or global compliance strategies

A second challenge that businesses highlight is the difficulty of elaborating a regional or global compliance strategy, even across countries that share common principles for data protection.

Practitioners consistently note that implementation approaches may vary significantly even where data transfer provisions appear consistent (e.g. subsequent guidance or subsidiary legislation may be more prescriptive on the approach to obtaining consent in one jurisdiction versus another), particularly in regions where no institutional mechanism of cooperation is available to ensure some degree of coordination. Moreover, cross-border compliance strategies involve not only compliance with the provisions on data transfers but also with all other substantive provisions of each law. These challenges are particularly high in regions like the Asia-Pacific (ABLI, 2020[23]) or Latin America, where the data protection landscape is fast evolving.

Organisations take different approaches to compliance for different reasons. In regions where legal variations are great, for instance, there is now a proven process of taking a GDPR compliance programme as the basis, then adjusting for elements that have no application in the relevant jurisdictions or for additional elements needed to achieve compliance (Hogan Lovells, 2022[24]). However, while some of the adjustments needed may be minor, others may be significant due to differences in substantive provisions or divergence in their interpretation, such as on legal bases for processing (in jurisdictions where the concept exists), on the definition of personal data, on transparency and consent requirements, on the age of children consent, or on the appointment of local representatives.

The variations between these are a source of costs, not only because of the need for formalisation of compliance at the legal level but also because of the need for differentiated information technology (IT) developments, some of which may be impossible to implement.[5] These differences can have tangible cross-border effects and strain compliance activities – to the point, reportedly, of discouraging the deployment of services abroad for some companies.

4.3. Businesses fear that the current regulatory environment might lead to ineffectiveness of compliance requirements

In this evolving context, nearly six in ten privacy professionals report that complying with cross-border data transfer laws is their most difficult task (IAPP-EY, 2021[25]). While they acknowledge that countries operate in different contexts and approach data protection issues from different perspectives, businesses express a shared concern that their own legal, financial or technical capacity for facing the current regulatory environment may be limited (Brazilian Internet Steering Committee, 2021[26]), and it may challenge the feasibility and effectiveness of compliance.

Increasing complexity, uncertainty and costs, together, risk creating compliance fatigue. Some businesses even suggest that the global regulatory ecosystem may lead to a paradox where data protection and privacy expectations have never been higher but where firms will progressively accept having to take a calculated risk of non-compliance. This may involve the deliberate choice of management to implement a procedurally oriented approach aiming at limiting enforcement risks rather than aiming for effective data protection outcomes first. This approach can include focusing compliance efforts only on countries or issues of strategic importance to them before considering extending this compliance to jurisdictions of lesser importance from their business perspective or before focusing on real risks to individuals' privacy and data protection.

There are also asymmetries in the capabilities of organisations to go through long and costly procedures required by some transfer mechanisms. These asymmetries can further entrench the advantages of larger and better-resourced companies. As budgets tighten in a context of a looming economic crisis and expenses to address other multiple types of risks also increase, some privacy professionals are alert to the risk that they will increasingly be asked by their management to arbitrate between the costs of compliance and non-compliance.

Business stakeholders are concerned that this might undermine the legitimacy and credibility of data protection rules, the role of compliance and data protection staff, and, more fundamentally, the effectiveness of protection for individuals. This means holding companies back from leveraging the trust-building capacities of national laws to the full, if at all, frustrating the companies' capacity to address other important risks they need to manage and invest resources in, such as cybersecurity or risks of algorithmic bias and discrimination. Others go further to suggest that an overly stringent approach to data transfer rules might create a hostile environment for investments. Ultimately, businesses generally express a concern that these factors combined create obstacles to building trust globally and bear a cost for society as a whole.

5 Businesses want means to carry out responsible cross-border data flows and meaningful data protection

5.1. Businesses support a diverse toolkit of policies and regulations that can be tailored to each business needs

Companies insist that their sizes, business models, data-processing operations, resources, and economic, cultural and social realities are diverse and that they need to be able to choose among different legal bases and transfer mechanisms to accommodate this diversity (CIPL, 2017[27]). That should include at least those of the diversified "toolkit" of mechanisms offered by the reform of the EU data protection legislation in 2016 (European Commission, 2017[28]). This is particularly important for SMEs, given their limited specialist resources and financial capacity to use third-party support on data protection.

In addition, companies support international arrangements that advance regional and cross-regional solutions for cross-border transfers. For instance, there remains interest in efforts to explore bridging the EU Binding Corporate Rules (BCRs) and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, which is now in the process of expanding into a new Global CBPR System beyond APEC. While the discussions on the interoperability of the CBPR System and BCRs have not been conclusive so far, the interoperability of other solutions building on commonalities between data protection laws could be explored in other contexts, such as between model or standard clauses from different regions or jurisdictions (such as the European Union, the Association of Southeast Asian Nations [ASEAN], the Ibero-American Network, etc.) or of certifications (possibly including CBPR), codes of conduct, BCRs or adequacy decisions to increase their network effect.

Such possibilities are supported by companies because they would reduce the time and effort required to negotiate and enable cross-border data transfers between business counterparts while allowing them to devote those same resources to streamlining and strengthening accountability measures and data protection programmes internally.

5.2. Businesses want an approach that focuses on substantive protection over formal compliance in the implementation of cross-border data transfer provisions

Businesses emphasise that they would like to avoid an excessively formal, paperwork-based approach to the implementation of cross-border data transfer provisions. This is necessary to minimise complexity and

costs, which might otherwise undermine the advancement of the protection of individuals' rights and the generation of trust intended by the spirit of the rule.

Companies confirm the need to put in place appropriate measures to deal with the privacy risks that exist in cross-border transfers of data. At the same time, companies perceive the risk of a universal trend towards "pro forma" compliance, potentially leading to unnecessary costs, diversion of resources from substantive data protection measures, including education and training, negative perception of data protection internally, loss of interest and of support from senior management, and demotivation of the privacy teams, among others.

Some businesses express a concern that focus on formal compliance procedures can distract governance attention from the development and implementation of privacy protective safeguards and associated controls in verifiable privacy management programmes of work. This type of risk is mentioned in different configurations around the globe. In one example, companies questioned the substance of the protection in default requirements to obtain "separate consent" from individuals for data transfers. Privacy professionals experience the addition of "another box to tick" more as a technical and operational constraint, interfering with user interface and experience, than as an effective form of personal protection. Moreover, the increasing use of individuals' consent in personal data protection regulation has contributed to devaluing the concept and, with it, the perception and attitude toward data protection rules, which may end up appearing as a series of checkboxes.

In another example, companies refer to positive obligations on them to carry out their own assessments of the data protection framework in the countries of destination of the data. This typically leads them to choose other legal bases or mechanisms for transferring data overseas, if possible. In jurisdictions including the EU since the Schrems II decision, a similar requirement also applies to companies regarding assessing foreign governments' laws and practices in accessing personal data held by the private sector. In any configuration, consistent feedback is that even the biggest companies do not have by themselves the capacity to analyse specific fields of regulation and monitor it over time on a global scale, including due to the lack of consistent information and knowledge sharing to assist with the task.

Lastly, companies and privacy counsels note that procedural formalities foreseen in some regulations, such as individual assessments and approvals, may give companies a "seal of approval" that is valued in a commercial context and provides an opportunity for reviewing their data practices. However, they note that these same procedures can lead to negative effects when the actual capacities of data protection regulators prevent those processes from being carried out swiftly and effectively. This also means the competent authorities must be given the means to issue guidance, process and hand down decisions within a reasonable timeframe to ensure equal treatment of all companies and organisations engaged in similar processes. Companies suggest that laws and policies could provide a greater margin of manoeuvre to data protection regulators to carry out their duties in line with the funding and staffing resources available, particularly in institutional contexts that are not well developed yet. More broadly, companies and legal counsels underline that continuous mutual dialogue between companies and regulators proves to be a helpful path forward to identify workable solutions for trustworthy data transfers and strengthen compliance in practice.

Exploring ways forward, companies suggest that regulatory mechanisms and tools are most effective when they require demonstrable and verifiable operationalisation in technology and organisation. For example, they thus suggest that it might be helpful to propagate some of the common regulatory tools into (International Organization for Standardization [ISO] or other) standards, as it would allow for a practical implementation that can also be verified on the ground. They go even further to suggest that that would be an effective way to assess the extent gaps or risks still exist that may be less recognised today due to their lower probability of verification.

5.3. Businesses ask for solutions that match their realities and support overall data protection strategies

Companies and their legal counsels suggest that some characteristics of cross-border data transfer tools make them particularly useful to strengthen companies' internal data protection strategies broadly, thereby helping to secure senior management buy-in, long-term commitment to those rules and principles and even competition benefits.

Companies are particularly keen on mechanisms, tools and legal bases for data transfers that generally follow the essential elements of accountability and can be leveraged with internal privacy management programmes and compliance infrastructures (including governance mechanisms, data protection officers, policies and procedures, training and communication, and audits and assessments). Companies favour tools that they can deploy and scale swiftly and flexibly across complex digital supply chains. In this regard, businesses suggest that strong internal compliance programmes can drive companies to *de facto* harmonise data protection across the globe, taking as reference the most stringent provisions in different countries.

A tool that is seen to hold potential to this effect is BCRs. BCRs were developed in the early 2000s jointly by the EU data protection authorities and large corporate groups at their request; they are now recognised in many data protection frameworks globally. Depending on their configuration, tools based on the principle of certification and codes of conduct, including the future Global (currently APEC) CBPR, can also be placed in this category.

However, the experience of BCRs shows that a condition for maintaining a positive assessment of these tools by companies is that these be scalable and efforts required to carry out the necessary formalities remain proportionate to the derived benefits.

5.4. Greater dialogue on the role of PETs is needed

While the understanding of what a privacy-enhancing technology is can vary, PETs generally refers to digital technologies, approaches, and tools that permit processing, analysis and sharing of information while protecting the confidentiality, and in some cases also the integrity and availability, of personal data (OECD, 2023[14]).

The business case for PETs is often focused on addressing risks through data minimisation or obfuscation, better mapping an understanding of data assets and data flows, and enabling proportionate data sharing rather than on cross-border data transfers specifically, being also aware that today PETs are generally not an alternative to legal and regulatory protection of data transfers for personal data but as an important tool to ensure more trustworthy data governance globally.

At the same time, businesses and legal counsels consider that there would be potential to advance in the context of DFFT through specific types of PETs, such as synthetic data, homomorphic encryption, differential privacy or tokenisation. They suggest that greater dialogue is needed around concepts such as anonymisation, de-identification and pseudonymisation of personal data.

Most companies indicate that it can be difficult to make investments in PETs because the costs may not be perceived as justified in an environment where a few policy makers and regulators have taken a stance on how to reap the full potential of PETs so far, as regulators have generally recommended deploying PETs as an addition to other existing requirements.

Against this backdrop, while recent developments of some PETs are considered promising, companies report that it is not clear whether investing in PETs would adequately address risks in cross-border scenarios and whether they constitute sufficient safeguards under multiple laws and regulations. This

assessment might change in the longer term, particularly if regulatory assessments in this space become available and more conclusive in their findings.

6 Existing legal bases and mechanisms for cross-border data flows could be further leveraged to advance DFFT

Over the years, similar but slightly varying mechanisms and legal bases for transferring data abroad have developed in data protection laws across the world (OECD, 2022[2]; Casalini, López González and Nemoto, 2021[5]). Below, some of the transfer mechanisms and legal bases that companies and legal counsels cite more frequently are discussed, highlighting the companies' perceptions of their potential for advancing trust in data flows.

While each transfer mechanism and legal basis has both strengths and limitations, businesses generally suggest that:

- Some transfer mechanisms and legal bases are more mature than others: the low pick-up rate of some of them today is not necessarily indicative of limited potential but could be due to the time needed to consolidate into a business case, the entry burden or the slow approval process.
- Cultural differences may play a role in companies' preferences, in particular, variable approaches to liability and risk. For example, legal counsels indicate that optional or voluntary accountability measures that involve a measure of regulatory scrutiny (approvals or assessments) might not be attractive for companies that operate in heavily regulated environments or in jurisdictions marked by a litigation culture where senior management tends to be more cautious about exploring or adopting new approaches.
- Solutions offered by governments and authorities could better accommodate evolving business priorities – e.g. solutions that fit with the implementation of their privacy management programmes (PMPs) or with global emerging standards.

6.1. The accountability principle applied to cross-border data transfers

Businesses generally consider the regulation of data flows through the so-called accountability principle, as it is stipulated, for instance, in jurisdictions including Australia (OAIC, 2020[29]) and Canada (OPC Canada, 2012[30]; justice.gc.ca, 2000[31]), as helpful. In general, the accountability principle in both countries puts the onus on the business transferring data to ensure that recipient organisations handle personal information consistently with the requirements of the law that applies to the transferring business. In Canada's case, this requirement applies whether the personal information is transferred to an organisation in another country, in another Canadian province, or in the same city. To ensure this consistency, organisations may use contracts or "other means". To strengthen accountability, some data protection regulations also have provisions requiring organisations (public and private) to appoint a data protection

officer (DPO) and offer communication channels to data subjects and regulators in matters of data protection in any country where they offer services.

Applying the rule of accountability to protect cross-border data transfers fosters trust as it provides for a protection that is highly context-specific. Data exporters carry quasi-vicarious legal liability risk if they get the specific compliance risk management and mitigation wrong. Businesses note that not all data transfers entail equal risks and harms for individuals and their privacy, and accountability is seen as providing legal incentives for companies to manage "end-to-end" risks for the data that they collect and handle, with a focus on substantive protection, regardless of geographical location or of the means used to uphold that protection.

Regulating data transfers by the accountability principle also ties in well with the many data protection laws that now have general provisions on accountability, which is a core principle of the OECD Privacy Guidelines (paragraph 14).[6] In this sense, some suggest that this approach could be particularly helpful in countries where data flow regulation is new or in the process of being built out, as it can help to maintain and encourage good practice and trust while regulators keep latitude to specify the conditions for implementation in specific guidance. This guidance can also adapt over time to new legal or technological developments.

On the other hand, to gain greater confidence on when and how to use this approach in a cross-border context, companies might need regulatory guidance, in particular, on which transfer tools effectively enable them to comply with the related requirement. In this sense, businesses have suggested that further work could be done on how accountability rules work in relevant jurisdictions and how accountability can be demonstrated via existing, evolving and new data transfer mechanisms, such as contracts, BCRs, standards and certifications, including CBPR. This would include considering the lessons that stakeholders draw from this approach, particularly about how regulators have interpreted these rules in practice.

6.2. Assessment of the level of data protection in destination countries ("adequacy")

Today, the assessment of the level of protection offered to data in a destination country is a building block of many data transfer regimes. Subnational governments may also have such assessment requirements, as in the case of Quebec in Canada.

Several data protection laws provide that data can be freely transferred to jurisdictions (be they country, territory, sector or international organisation) that have been formally recognised by a public authority as providing an "adequate", "equivalent", "equal or higher" or "comparable" level of protection compared with domestic laws ("positive lists" or "adequacy decisions" approach). Companies generally welcome the adoption of such adequacy decisions as a powerful trust-building element. In a complex geopolitical context, an adequacy decision from one country with respect to another is the manifestation of a form of trust that effectively supports the development of seamless data transfers, as well as holds the potential to alleviate the regulatory risks weighing on companies. In contrast, the option that public authorities would establish "negative lists" or "deny lists" of countries to which data cannot flow is generally seen as undesirable not only from a compliance perspective but also as increasing distrust in an environment already under severe strain.

Yet other countries have in force provisions requiring that the assessment of the level of data protection in destination countries be done by the exporting organisation on a case-by-case basis, without intervention from the supervisory authority. Companies and counsels challenge the feasibility of this option. As noted earlier, they assert that such broad assessments, which go beyond assessing the risks of the specific transfer, put a significant burden on them, especially as the necessary benchmarks, expertise and language skills may not be accessible, and risk assessments may become quickly obsolete due to fast-

changing circumstances in destination countries. Moreover, a desk-based assessment of a particular regime does not address issues such as actual compliance, enforcement or enforceability.

At the same time, businesses note some limitations of positive list approaches from a policy perspective. For example, there are concerns that political considerations might affect adequacy decisions, or that adequacy decisions may change (whether for political or substantive reasons), which impacts business decision making about how far they can forecast the regulatory environment.

Reflecting on adequacy decisions, businesses highlight that while there is often a large degree of convergence in relation to data protection laws across countries, there is significant variation in what is publicly available about government access to data and in the approaches that governments are taking in this area. In this regard, they underline the importance that the work done on these issues at the OECD be continued to consolidate the trust built among the stakeholders involved. As shown by the discussions at the OECD, challenges relating to government data access practices are relevant globally.

Many companies and legal counsels also note that the capacities of "smaller" or younger regulatory authorities are too limited to commit resources to maintain a register and monitor assessments of foreign laws over time. This can make it unrealistic for some countries to adopt an "adequacy" regulatory approach – other than through the automatic endorsement of adequacy decisions taken by other jurisdictions.

Nevertheless, business feedback indicates traction in developing the interoperability of data protection frameworks across the globe through positive adequacy findings. For example, the growing number of jurisdictions recognising the same foreign jurisdictions as providing adequate data protection can lead to the development of a broad network where data can flow freely. Mutual adequacy arrangements, such as the one concluded between Japan and the EU, can present similar benefits. From a business perspective, the more adequacy decisions there are, the better, although priority should go to countries between which flows are traditionally dense and sustained (regardless of the countries' size).

In this sense, some businesses suggest that governments should further leverage all the possibilities offered by this tool, such as partial adequacy decisions for certain regions or sectors. They also suggest that mutual recognition systems or a regional or multilateral approach might be helpful, including through mechanisms that would support a network of comparable adequacy decisions. This is provided that convergence is not done at the lowest common denominator ("any data protection law") but on common standards emerging from national data protection laws in order to promote trust.

6.3. Contracts

Many data protection frameworks recognise contractual arrangements or data transfer agreements as a valid approach to ensuring that data transferred abroad be subject to appropriate safeguards and as a valid means for an organisation to comply with cross-border data transfer obligations.

Back in 2000, the OECD noted that "the idea of using contracts for trans-border data flows has been around for some time", citing the Council of Europe Model Contract (1992), later revised by the International Chamber of Commerce (ICC) (OECD, 2000[32]). Indeed, contractual provisions belong to the standard safeguards that are often necessary in relationships between business partners to ensure compliance with given privacy policies and practices, including in a cross-border context.

The predominant role of contracts to frame cross-border data transfers comes up consistently to this day in describing companies' compliance programmes: "contracts are king"; standard contractual clauses (SCCs) are the "most favoured option" or even the "*lingua franca*" of data transfer tools. The International Association of Privacy Professionals (IAPP)-Ernst & Young (EY) Annual Privacy Governance Report 2021 confirms this feedback: 94% of firms transferring data from the European Union currently use EU SCCs as their primary legal basis (IAPP-EY, 2021[25]). In many countries where relatively new data protection

frameworks are in place and regulatory authorities are not fully operational, contracts are often also the only useful mechanism to comply at the moment.

Of all the existing tools, from a compliance perspective, contractual arrangements are perceived as providing the greatest legal certainty. Contracts are a "universally identified legal object" with relatively low maintenance costs that do not require recurrent revalidation and are easier to sell to management than more "prospective" or resource-intensive tools with fewer established business cases. In addition, additional standard clauses that must be included according to some laws or additional parties can relatively easily be integrated into larger framework contracts through docking clauses or annexes. According to legal counsels, the implementation of contracts is also currently seen as subject to less regulatory scrutiny than other compliance mechanisms, making them more easily acceptable by companies that are culturally averse to proactively engaging with the regulator.

Reflecting their wide use by business, different sets of prescribed contractual clauses have been developed by several jurisdictions or regional groups in recent years, including by the European Union, the United Kingdom (International Data Transfer Agreement, IDTA) (ICO, 2022[33]), New Zealand (together with a Model Contract Clauses Agreement Builder) (The Privacy Commissioner (NZ), 2021[34]), ASEAN (ASEAN, 2021[35]), the Ibero-American Data Protection Network (RIPD) (REDIPD, 2022[36]). In addition, work is ongoing to update the SCCs of the Council of Europe in light of Convention 108+.

Companies' feedback suggests significant traction in developing more regional solutions and in seeking to make contractual safeguards compatible between different jurisdictions and regions. The clauses in place today in different regions have different contents and formats and are not "grafted" onto identical legal regimes, which may limit their practical adoption. For instance, some jurisdictions do not recognise the distinction between controllers and processors, which is central in other jurisdictions. This has led to the drafting of separate model clauses that are not readily useable across different countries. However, work is ongoing (for instance between the European Union and ASEAN) to bridge different sets of model clauses to facilitate compliance with cross-border transfer rules for companies operating across different regions of the world.

In this context, also at a practical level, legal counsels assisting their clients in cross-border environments are trying to develop their own "contracts for the world" that provide the key provisions on which to anchor all the regional clauses, whether prescribed or optional, as needed. In 2022, the United Kingdom published an international data transfer addendum to the European Commission's SCCs for international data transfers, which can be used by companies to comply with the UK GDPR (ICO, 2022[37]). This approach was welcomed by companies, as they tend to use the EU SCCs and can thus practically add these clauses to comply with both regulations, in an example of the importance of interoperability.

In 2022, the Group of Twenty (G20) Digital Economy Working Group report highlighted the benefits that model contractual clauses could offer as a mechanism towards DFFT (G20, 2022[38]). The Global Privacy Assembly is also undertaking work to compare the different sets of contractual clauses across the world.

Notwithstanding the general recognition of contracts as a useful mechanism to achieve compliance even in complex situations, some companies and counsels mention the risk that the signature of contracts may be considered merely as a paper exercise. In other words, contracts may help to show compliance to regulators or commercial partners but may not always translate into practical compliance measures and greater protection for individuals and their personal data.

Companies advocate for the development of common and streamlined clauses directly related to accountability requirements. This is particularly needed as contract management is seen as particularly challenging to sustain in today's global digital economy. The day-to-day upkeep of clauses is reported as a significant endeavour as firms change or consolidate suppliers, onboard and offboard partners, upgrade systems, and so on. Drafting, processing, and executing contracts can draw significant human resources and even need to be outsourced at significant costs. Accordingly, companies find that the following would

be challenging developments for them: having more sets of regional clauses that include special requirements (e.g. specific annexes or data-mapping requirements); making the integration of such clauses into wider contracts less flexible; or amending such clauses without a sufficient grace period. They consider that such developments could, in practice, diminish the benefit of regional or local solutions, making the construction of a global contract-based compliance strategy more complex and unsustainable for companies. Therefore, companies call for scalable contractual solutions that could "bridge" different regional sets of model clauses.

6.4. Binding Corporate Rules

Binding Corporate Rules (BCRs), also referred to as internal or intra-group rules, are data protection policies adhered to by companies for cross-border transfers of personal data within a group of undertakings or enterprises (Robinson, Kizawa and Ronchi, 2021[4]). In general, they establish uniform internal rules for transferring personal data across a corporate group or a group of undertakings and are binding on all relevant entities and personnel in these groups. As such, they require a comprehensive privacy programme and compliance infrastructure, including governance mechanisms, DPOs, policies and procedures for, e.g. complaint handling, data subject access requests, methods of reporting to supervisory authorities, as well as training and communication, audits and assessments, and others.

BCRs are recognised (and could be recognised) as a valid data transfer mechanism in most countries where data transfer provisions laws are in place. In the European Union and the United Kingdom, where the concept was originally developed at the initiative of business together with the predecessor of the EDPB, BCRs also require approval by the regulator in each EU member state in which the organisation will rely on them to comply.

Businesses are supportive of the BCRs tool in principle as a form of certification and accountability mechanism. BCRs are a form of certification that can be adapted to the specificity of companies that need to transfer data within a corporate group or among companies involved in a joint economic activity. . In jurisdictions that require prior approval, companies that have obtained approval for their BCRs use them to demonstrate their holistic commitment to data protection and compliance internally and externally. Once a company has BCRs in place, they no longer need to enter lengthy contract negotiations or complex paperwork (at least with regard to the processing operations that the BCRs cover). It helps to simplify and accelerate compliance processes, which is valuable for businesses.

Some companies that are EU BCRs-certified go even further to suggest that the importance of this tool might not be completely understood yet by industry and even less by individuals and investors. In this sense, they suggest that smaller companies might be more willing to undertake the BCRs approval process if they could get a "seal" or "trustmark" that is more widely recognised. Companies whose BCRs have been approved strongly back the idea that the mutual recognition of BCRs in multiple jurisdictions be facilitated to advance DFFT.

At the same time, a majority of businesses point out that in practice today, in some jurisdictions where it is required, the regulatory approval process tend to be long, expensive and challenging overall, requiring time and continued legal fees to support the process. Regulators expect documentation in a form that they understand but which does not necessarily match the companies' own data governance formats, culture and approach, leading to a duplication of efforts, going against the approach initially taken to the tool. As privacy regulators are very stretched with their other compliance and enforcement work, many suggest that an option might be to empower trusted third parties to approve and audit BCRs on behalf of Data Protections Authorities, in a "charged for" co-regulatory model, similar to the regulatory model of certification.

Up until now, the use of BCRs does not seem to have been actively promoted outside of the European Union and the United Kingdom, possibly due to the perception that BCRs are a solution that cannot be readily transposed in other countries. Yet feedback suggests that the magnitude of BCRs effectively operated outside the European Union and the United Kingdom is still underestimated. This is because the tool is not subject to approvals outside the European Union or the United Kingdom, and therefore its use to satisfy data transfer requirements is difficult to assess with precision. Subject to appropriate reflection on the administrative aspects, therefore, the expansion of BCRs into more jurisdictions could be explored.

In all contexts, companies suggest that future developments in the space of BCRs should strive for a mix of clear, efficient and transparent *ex ante* and *ex post* regulation and processes that allow for balancing the upfront investment to undergo regulatory assessment and putting in place new corporate guidelines with ongoing support and supervision, possibly involving third parties.

Companies and counsels suggest several areas for improvement. Overall, they would welcome the re-incentivisation of BCRs by regulatory authorities, in particular, by setting up more resources or by simplifying the approval process when it exists, in recognition of the fact that they directly translate into better data protection practices. Moreover, there needs to be a critical mass of countries recognising the tool to extend its relevance into more jurisdictions and to explore commonalities across different BCRs and how future mutual recognition of BCRs across borders could be possible. Some business representatives go even further to suggest that it might be possible to evolve BCRs to act as a transfer mechanism between corporate groups holding BCR approval. Both corporate groups would be deemed as “adequate destinations” for data coming from each other, given their BCR-approved status.

6.5. Certifications

Companies look at privacy certifications in data protection laws, including data protection seals and trustmarks, as valuable elements in their accountability framework for data protection. Privacy certification schemes allow organisations to demonstrate compliance with some or every national data protection requirement to individuals, regulators and business partners. In this sense, they can also be understood as a competitive business advantage (or as a competitive disadvantage for companies that do not have it when certification has become a generally established market feature).

In some countries, being certified with a scheme recognised by the data-originating country also enables companies to comply with obligations for cross-border data transfers. Today, relatively few jurisdictions have effectively taken the necessary steps for companies to use certification (as well as codes of conduct) as a transfer mechanism, but many of them could do so in theory.

The businesses consulted are divided on the merits of certification. For some, there is great potential for such schemes if processes are improved, in particular, because they may solve some interoperability issues. In contrast, others express a concern that these schemes might fuel a market whose economic model favours the development of costly, standardised and renewable processes that focus on formal compliance rather than on substantive protection. Feedback suggests that some companies go through the initial phase of the certification process but do not seek to obtain the actual certification, as they consider that they have done enough by assessing their practices and having built awareness. The saved budget is then spent on other priorities, such as privacy training, while continuing to use contracts for transfer compliance.

Until now, the future Global (currently APEC) CBPR and Privacy Recognition for Processors (PRP) systems have been the most frequently cited examples of certification schemes for cross-border data transfers. In practice, they are the only certification-based transfer mechanism in operation today. Based on the nine APEC Privacy Principles developed in the APEC Privacy Framework, the certification works through voluntary, principles-based privacy certification mechanisms for data controllers (and, in the case

of the PRP, for data processors) in participating member economies. The CBPR System relies on third-party agents ("accountability agents", AAs) to guarantee the certification, be they either public bodies (e.g. in Singapore or Korea) or private entities (e.g. in the United States or Japan).

Until now, the take-up of the APEC CBPR System has been relatively low at the company level. The reasons provided by companies are diverse. One factor is that the costs of obtaining and renewing certification are relatively high. In addition, CBPR does not displace the domestic law of a participating economy, meaning it does not always represent compliance with applicable local data protection and privacy laws. Companies suggest that clarifying the interrelationship between CBPR and the applicable local privacy laws would be important, especially to ensure the benefits of the certification outweigh its costs (human and financial costs, as well as liabilities incurred).

A "network effect" as more jurisdictions join the same certification scheme would also be seen as strengthening the business case for this type of mechanism. In this regard, companies have expressed an interest in the evolution of APEC CBPR towards "Global CBPR", announced in April 2022, which will allow participation by jurisdictions without geographic limitation based on a consensus decision by all Global CBPR Forum members. The Global CBPR Forum is set to fully operationalise in spring 2023 and intends to establish an international certification system based on the APEC CBPR and the related Privacy Recognition for Processors (PRP) Systems. Once established, the Global CBPR System will be substantially similar to the APEC CBPR System in structure and technical requirements, but the system will be independently administered and separate from APEC. However, companies are currently awaiting clarification on the consequences of this development, in particular as to whether the APEC CBPR System will be definitively replaced by the Global CBPRs or whether the two systems will co-exist.

There have also been important developments in the area of certification in the European Union, where certification features among the appropriate legal bases that may be used by data exporters for transfers to third countries. In February 2023, the EDPB adopted two guidelines on certification (EDPB, 2023[39]) and Codes of Conduct (EDPB, 2022[40]) as tools for transfers, so as to provide guidance on these transfer mechanisms, which share many commonalities. The guidelines complement Guidelines 01/2018 on certification, which provides more general guidance on certification. No certification body has yet been accredited to grant the certification in the European Union, although development in that sense is expected to take place soon.

Companies express interest in seeing what, if any, link could be developed between the EU certification frameworks and the CBPR System, whether APEC or Global.

Companies also report that a somewhat under-explored certification system for data transfers might be around the standards of the ISO, namely ISO 27701, which extended the ISO information security management systems to cover the specificities of the processing of personal data in August 2019. Companies that are ISO 27701-certified argue that this advanced and well-established form of certification could be further leveraged by being recognised as a valid means for ensuring sufficient data protection guarantees in cross-border data transfers.

Finally, companies mention a series of additional considerations as relevant to build a stronger business case to stimulate the uptake of certifications as accountability tools and/or transfer mechanisms. These include the definition of "what" or "who" will be certified in the first place (organisations, PMPs, products, processes or services, or parts of those). The "quality" of the certification will also be conditioned by the criteria for the accreditation of certification bodies to ensure equality in independence, competence, adequate resourcing and accountability. Lastly, the potential for the scheme to work together with other standards, and its scalability for application to organisations of different sizes and types, are considered crucial by businesses.

6.6. Consent

Consent has long been a “default option” for cross-border data transfers in many jurisdictions, for lack of a better option available, particularly when companies operate in a fragmented legal environment where consent appears to be the only common building block of several data transfer regimes. This solution has spread by default and businesses report that regulators have so far shown a willingness to accept consent as a formal tick-the-box exercise in some jurisdictions.

However, jurisdictions increasingly move in the direction of recognising that consent must be freely given, specific, and informed but also “revocable” or “capable of being withdrawn” to be valid. The trend towards revocability of consent makes it difficult for companies to use it as a legal ground for recurring transfers unless organisations have twin servers, one onshore and one offshore, to allow individuals to toggle between where they want their data – which is not how they are setting themselves up.

To that end, companies suggest that lawmakers refrain from requiring consent in all circumstances and focus on providing solutions that guarantee substantive protection. They also note that in most cases, consent for data transfers should not apply as it does not afford real protection for data once they are transferred to another country, as actual transfer mechanisms do.

In the current context, companies indicate that at least there should be greater coherence across the conditions for consent-based transfers in different legal systems, including with regard to consent withdrawal, content of notices, or what qualifies as “express consent”. In particular, the level of detail of information provided to the individual and the methods of providing those should be addressed not in the law itself but preferably in guidance issued from a dialogue between relevant stakeholders, which could factor in the risk of conflict between different consent requirements.

7 Conclusion

Consultations with businesses confirm a shared interest of a growing number of OECD countries and partner economies to foster trust and facilitate cross-border data flows. This interest is attested by the exponential development of data protection laws around the world, which often share many commonalities and elements of convergence (OECD, 2022[2]). At the same time, businesses report that they are struggling to comply with an increasing number of obligations required of them as the natural corollary of such development of data protection laws globally. In other words, the challenge does not lie with the existence of data protection laws as such, which are a critical element of trust. But the constraints attached to the cumulation of multiple compliance obligations, even when stemming from comparable or even identical principles, can be such as to undermine the very purpose that each regulation intends to serve.

Moving forward on DFFT requires an integrated policy approach, both domestically and internationally, to build trust. Governments and regulators, including privacy regulators but also sectoral regulators, need to co-operate across silos, borders and at different levels simultaneously to support companies in their efforts to build trust and multi-jurisdictional compliance. Overall feedback suggests that the impact of cross-border data flows on other policy objectives depends both on a variety of domestic policy settings and on the nature and degree of international regulatory co-operation on data and data flows. As the report shows, solutions exist to bridge different privacy and data flows regulatory systems and facilitate DFFT. As regards some of these solutions, in particular, businesses welcome the current impetus to further expand them into scalable solutions at the regional and global level.

Based on these business consultations, DFFT advancement focused on data protection and privacy could be facilitated by:

- **Enhanced dialogue**: Providing policy makers with information relating to DFFT. This information could cover business experiences, policy and regulatory developments, use cases good practices and examples of solutions, including technological solutions, in place in the business community. They should include actors that have proven expertise in analysis, metrics and measurements in the area of data protection, including the OECD and the Global Privacy Assembly. It could also include the experience of the ISO in implementing the ISO 27701 standard, among others.
- **Greater legal certainty**: Building trust through domestic policies that are transparent, predictable, consistent across sectors and focused on outcomes – meaning aimed at providing effective protection to individuals, instead of cases where formalities-oriented compliance solutions do not necessarily contribute to effective data protection.
- **Further incentives for a culture of global compliance and trustworthiness among businesses**: Fostering and incentivising a global privacy and data protection culture for companies built on shared principles, compliance, organisational accountability, streamlined processes and a strong business case for a range of complementary transfer mechanisms.
- **International regulatory co-operation on privacy and data protection**: Building a coherent global regulatory landscape leveraging the full range of options for international regulatory co-operation to ensure a high standard of data protection and uphold trust around privacy and data protection globally. Such efforts should build on the experience of a range of stakeholders across different disciplines, sectors and levels of government and a common framework to address these issues holistically.

Annex A. Stakeholders consulted

The authors would like to thank private sector stakeholders who have contributed their time and expertise to provide input for this report (in alphabetical order):

- David Alfred, Director and Co-Head, Data Protection, Privacy and Cybersecurity Practice, Drew & Napier LLC (Singapore)
- Ruth Boardman, Partner, Bird & Bird (United Kingdom)
- Simon Hania, Senior Director of the Data Protection Office and Global Data Protection Officer, Uber (Netherlands/United States)
- Mercy King'ori, Lead Policy Analyst – Africa, Future of Privacy Forum (Kenya)
- Danny Kobrata, Partner and Founder of the Corporate and Technology Practice, K&K Advocates (Indonesia)
- Phil Lee, Managing Director, Digiphile Services Ltd (United Kingdom)
- Peter Leonard, Principal and Director, Data Synergies Pty Limited (Australia)
- Caroline Louveaux, Chief Privacy Officer, Mastercard (Belgium) and Derek Ho, Senior Vice President, Assistant General Counsel, Privacy and Data Protection, Mastercard (Singapore)
- Melody Musoni, Senior Subject Matter Expert: Data Protection, IBF International Consulting, Southern African Development Community (SADC) Secretariat (Botswana)
- Fabrice Naftalski, Partner, Global Data Privacy Law Leader, Head of IP/IT/Digital Law Practice Paris, E&Y Law (Ernst & Young) (France)
- Karima Noren, Co-founder, Privacy Compliance Hub (United Kingdom)
- Yann Padova, Partner and Head, Data Protection Practice, Baker McKenzie (France)
- Kwang Bae Park, Partner and Head of the Technology, Media and Telecommunications group, Lee & Ko (Korea)
- Mark Parsons, Partner and Head of Asia-Pacific region regulatory practice, Hogan Lovells (Hong Kong, China)
- Deepak Pillai, Partner, Christopher & Lee Ong (in association with Rajah & Tann Singapore LLP) (Malaysia)
- Paulo Marcos Rodrigues Brancher, Partner and Jacqueline Simas de Oliveira, Senior Associate, Mattos Filho (Brazil)
- Takeshige Sugimoto, Managing Director and Partner, S&K Brussels LPC (Japan)
- Omer Tene, Partner, Goodwin (United States)
- Eduardo Ustaran, Partner, Global Co-Head of the Privacy and Cybersecurity practice, Hogan Lovells (United Kingdom)
- Daimhin Warner, Principal and Director, Simply Privacy (New Zealand)
- Dino Wilkinson, Partner and Masha Ooijevaar, Senior Associate, Clyde & Co (United Arab Emirates)

The authors also would like to thank the following organisations for their comments:

- **Centre for Information Policy Leadership (CIPL)**: Bojana Bellamy, President, Natascha Gerlach, Director of Privacy Policy and Vivienne Artz, Officer of the Most Excellent Order of the British Empire (OBE), Data Strategy and Privacy Policy Advisor
- **International Association of Privacy Professionals (IAPP)**: Caitlin Fennessy, Vice-President and Chief Knowledge Officer and Isabelle Roccia, Managing Director, Europe
- The members of the **Privacy Law Working Group (PLWG) of the International Association of Transportation Airlines (IATA)**.

The authors also recognise all other stakeholders who contributed their perspectives and are not mentioned according to their confidentiality preferences.

The stakeholders consulted were selected by the OECD Secretariat based on the following criteria:

- **For all stakeholders**: Regional diversity (including European Union and United Kingdom, North and Latin America, India, Southeast Asia, Hong Kong [China], Japan and Korea, Middle East, and Africa).
- **For companies**: Sectoral diversity (including ICT, e-commerce, retail, food, oil and gas, civil aviation, cloud computing, life sciences, automotive, online payments, multi-service digital platform and fintech, financial industry), as well as size and market footprint (either regional, sub-regional or global).
- **For legal counsels**: Regional coverage; breadth of expertise; pools of clients (covering more than 200 companies in total, in all regions); established work relationships with national regulators.

The profiles of corporate representatives include general counsels, chief compliance officers, chief privacy officers or regional privacy teams of company groups based in Europe (including the European Union, the United Kingdom and Switzerland), North America, Latin America, Southeast Asia and Asia-Pacific.

Views expressed by stakeholders are reported to the extent that they were shared by several contributors. Single opinions have not been used when their representativeness could not be established.

All the experts who were contacted to contribute to this study agreed to share their experiences.

References

ABLI (2020), *Transferring Personal Data in Asia: A Path to Legal Certainty and Regional Convergence*, https://fpf.org/wp-content/uploads/2021/01/Girot_Transferring.pdf. [23]

ASEAN (2021), *ASEAN Model Contractual Clauses for Cross Border Data Flows*, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. [35]

Brazilian Internet Steering Committee (2021), *Privacy and Personal Data Protection, Perspectives of Individuals, Enterprises and Public Organisations in Brazil*, https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. [26]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://doi.org/10.1787/b2023a47-en. [6]

Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en. [5]

Chevalier, S. (2022), *U.S. consumer distrust in shopping recommendations 2019, by platform*, https://www.statista.com/statistics/1041531/distrust-in-shopping-suggestions-digital-platforms/ (accessed on 2022). [3]

CIPL (2017), *Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy*, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf. [27]

Digital Agency, Japan (2022), *Overview of DFFT*, https://www.digital.go.jp/en/dfft-en/. [7]

EDPB (2023), *Guidelines 07/2022 on certification as a tool for transfers*, https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf. [39]

EDPB (2022), *Guidelines 04/2021 on Codes of Conduct as tools for transfers*, https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf. [40]

European Commission (2017), "Communication from the Commission to the European Parliament and the Council", *Exchanging and Protecting Personal Data in a Globalised World*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN. [28]

Federal Ministry for Digital and Transport (2022), *G7 Action Plan for Promoting Data Free Flow with Trust*, G7 Digital Ministers' Track - Annex 1, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile (accessed on 11 January 2023). [15]

G20 (2022), *G20 Bali Leaders' Declaration*, https://www.g20.org/content/dam/gtwenty/gtwenty_new/about_g20/previous-summit-documents/2022-bali/G20%20Bali%20Leaders%27%20Declaration,%2015-16%20November%202022.pdf. [38]

Global Data Alliance (2022), *Sectors*, https://globaldataalliance.org/sectors/. [17]

Global Privacy Assembly (2022), *Other Networks*, https://globalprivacyassembly.org/other-networks/ (accessed on 2022). [20]

Greenleaf, G. (2023), *Global data privacy laws 2023: 162 laws and 20 bills*, https://www.privacylaws.com/reports-gateway/articles/int181/int181_2023/. [19]

Hogan Lovells (2022), *Asia Pacific Data Protection and Cybersecurity Guide 2022*, https://f.datasrvr.com/fr1/022/16167/APAC_Data_Protection_and_Cyber_Security_Guide_2022.pdf. [24]

IAPP-EY (2022), *IAPP-EY Annual Privacy Governance Report 2022*, https://iapp.org/resources/article/privacy-governance-report/. [41]

IAPP-EY (2021), *IAPP-EY Annual Privacy Governance Report 2021*, https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf. [25]

ICO (2022), *International Data Transfer Agreement and Guidance*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. [37]

ICO (2022), *UK's International Data Transfer Agreement*, https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf. [33]

IRSG (2022), *The Future of International Data Transfer*, https://www.irsg.co.uk/assets/Reports/AA_IRSG_DataTransfers_05.pdf. [22]

justice.gc.ca (2000), *Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5)*, https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-7.html#h-417659 (accessed on 11 April 2023). [31]

López González, J., F. Casalini and J. Porras (2022), "A preliminary mapping of data localisation measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris, https://doi.org/10.1787/c5ca3fed-en. [8]

OAIC (2020), *Part 7: Organisational accountability requirements for entities*, https://www.oaic.gov.au/privacy/the-privacy-act/review-of-the-privacy-act/privacy-act-review-issues-paper-submission/part-7. [29]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [14]

OECD (2022), *Cross-border Data Flows: Taking Stock of Key Policies and Initiatives*, OECD Publishing, https://doi.org/10.1787/5031dd97-en. [1]

OECD (2022), *Declaration on Government Access to Personal Data Held by Private Sector Entities*, OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487. [11]

OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, https://doi.org/10.1787/139b32ad-en. [2]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463. [13]

OECD (2020), *Regulatory Impact Assessment*, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, https://doi.org/10.1787/7a9638cb-en. [21]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en. [12]

OECD (2000), "Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks", *OECD Digital Economy Papers*, No. 66, OECD Publishing, Paris, https://doi.org/10.1787/233311170363. [32]

OECD (forthcoming), *OECD Privacy Guidelines Implementation Guidance: Draft Chapter on Accountability*. [42]

OECD (forthcoming), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Privacy Laws*. [10]

OPC Canada (2012), *Getting Accountability Right with a Privacy Management Program*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/. [30]

REDIPD (2022), *Publicación de la Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales*, https://www.redipd.org/es/noticias/publicacion-guia-implementacion-clausulas-contractuales-modelo-para-tidp. [36]

Robinson, L., K. Kizawa and E. Ronchi (2021), "Interoperability of privacy and data protection frameworks", *OECD Going Digital Toolkit Notes*, No. 21, OECD Publishing, Paris, https://doi.org/10.1787/64923d53-en. [4]

Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris, https://doi.org/10.1787/7fbaed62-en. [9]

The Privacy Commissioner (NZ) (2021), *Model Contract Clauses Agreement Builder*, https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/. [34]

UNCTAD (2021), *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed on 2022). [18]

UNCTAD (2021), *Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow*, https://unctad.org/system/files/official-document/der2021_en.pdf. [16]

Notes

1. The list of experts and organisations consulted and the criteria for their selection are presented in Annex A of this report.

2. According to the IAPP-EY 2022 Privacy Governance Survey, international transfers of personal data are one of the top strategic privacy priorities for 2022 overall, especially in technology and telecommunications, business services, life sciences and healthcare, legal, and manufacturing (IAPP-EY, 2022[41]).

3. For the remaining 5%, the source reports “no data”.

4. Privacy budgets increased by 60% in 2021 and are expected to increase more (IAPP-EY, 2021[25]).

5. For example, in Asia Pacific, direct marketing regulation remains a patchwork, with technical requirements that are specific to each jurisdiction, whether under the data protection law itself or under anti-spam laws, Internet regulation or consumer protection laws.

6. Further guidance will soon be published in the form of a dedicated Chapter on Accountability in the Implementation Guidance for the OECD Privacy Guidelines (OECD, forthcoming[42]).