CONSUMERS INTERNATIONAL

COMING TOGETHER FOR CHANGE

RECOMMENDATIONS FOR INTEROPERABLE & CONSUMER-CENTRIC REDRESS IN THE EVENT OF PERSONAL DATA MISUSE IN INTERNATIONAL DATA-TRANSFERS

CONTENTS

SUMMARY

Cross-border data flows have become essential to the functioning of the global digital economy. They underpin social interactions, international business operations, logistics, supply chains and global communication. Critical in enabling more seamless, controllable and transparent cross-border data flows has been the development of harmonised legal frameworks. A large part of data crossing borders is personal data, subject to the more rigorous protection provided by personal data legal frameworks. However, in the context of international personal data transfers (IPDTs), and despite these enhanced protections, there is still significant risk to consumers that their personal data will be misused, and further, where regulatory frameworks are incompatible, that consumers' access to redress will be limited. With the majority of global data processing taking place in upper-income countries, and with the volume of data being processed only likely to increase in the future, robust redress mechanisms that serve consumers regardless of where in the world they live are a growing priority.

This report reviews and evaluates current options for consumers to seek redress when personal data is misused in the context of IPDTs. The misuse of personal data means any non-compliant processing of personal data. Common examples of personal data misuse include breach of personal data, collection error (ie, an instance in which personal data is incorrectly or unnecessarily collected without a legitimate legal basis) and unauthorised use (when personal data is processed for a certain purpose, but is ultimately used by the data controller for another purpose). Redress means all available administrative and judicial remedies consumers may access to obtain compensation, or repair or restore a situation of data misuse. It also includes a consumer's rights as a data subject, such as rights to access, correction, erasure and objection, data portability, and the right to revoke consent.

This report reviews lawful mechanisms for IPDTs as they are represented in the following five legal frameworks: the European Union's General Data Protection Regulation (GDPR); the Council of Europe's Convention 108+; the Asia-Pacific Economic Cooperation (APEC)'s Privacy Framework;

the Standards for Personal Data Protection for Ibero-American Data Protection Network (RedIPD – acronym in Spanish); and the Brazilian General Data Protection Law (LGPD).

The lawful basis for international personal data transfers (referred to in this report as the IPDT mechanism) varies across these legal frameworks. Within the selected frameworks are four varying and sometimes overlapping IPDT mechanisms: adequacy decisions; standard contractual clauses (SCCs); certification; and consent.

Using the United Nations's *Guidelines for Consumer Protection* as a point of reference, the report reviews options for redress for consumers within each of these IPDT mechanisms, in each of the legal frameworks in which they appear. Then, drawing on existing literature, case studies and interviews conducted with stakeholders from different regions and areas of expertise, the report highlights challenges to consumer-centric redress, and opportunities for improved consumer outcomes.

The report ends by providing recommendations to policy-makers, regulators, civil society and industry for strengthening the protection of consumer rights, and bolstering the overall consumer experience.

The report unearths a significant gap between the theoretical protections offered by international data protection frameworks and the practical realities faced by consumers seeking redress internationally. The complexities of international data transfers, the fragmented regulatory landscape, and the inconsistent implementation of data protection laws contribute to the challenges consumers encounter in exercising their rights effectively.

Addressing these challenges will require a multifaceted approach. For state and public sector entities, establishing clear pathways for consumers to access their rights and engage with personal data protection authorities is crucial. This includes fostering agreements between national and international authorities to facilitate complaint resolution across borders, and developing informal conflict resolution mechanisms that provide alternative avenues for redress (which may be most effectively executed together with the private sector). Strengthening collective redress mechanisms should also be a priority.

The report highlights the need for regulatory interoperability, to ensure consumers achieve redress, through individual or collective means, and discusses current efforts around Data Free Flow with Trust (DFFT). It emphasises that interoperable regulations have to be constructed bringing into consideration each jurisdiction's particularities, geopolitical position and, crucially, acknowledging consumer vulnerabilities, which may vary in each region. It identifies digital sovereignty as a possible guiding principle to building interoperable frameworks that meet these criteria, enabling new initiatives to work towards interoperability in a manner that protects consumers and maintains a free and open internet, while based on the UN *Guidelines on Consumer Protection.*

The report further recommends that policy-makers and international organisations apply the highest possible consumer and data protection standards to promote equitable treatment of consumers across jurisdictions. This is an essential step towards mitigating disparities arising from varied national data protection laws. Increased regulatory interoperability through multilateral agreements and financial support for developing countries can help bridge the gap between different legal frameworks and jurisdictions, promoting a more cohesive global approach to data and consumer protection.

The report emphasises the need to engage not only global and local businesses of all sizes but also civil society and consumer protection bodies in the regulatory process, to enhance the effectiveness of regulations by incorporating diverse perspectives and local realities. Awareness-raising efforts, particularly through provision of transparent and appropriate information, will

further empower consumers to better understand and exercise their rights, especially when accompanied by ongoing investment in data privacy and security.

By adopting these recommendations, policy-makers, regulatory bodies, and industry leaders can strengthen the protection of consumer rights and ensure that options for achieving redress are both effective and accessible. This holistic approach will contribute to a more equitable and responsive data protection landscape, ultimately reducing complexity, while enhancing consumer trust and confidence in international data practices.

The protection of consumers' personal data rights is a critical concern in the context of IPDT. The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor. Because IPDTs have become integral to trade expansion and economic growth, it is imperative that the utmost care is taken to protect consumers, so as not to undermine confidence in the global economy.

RECOMMENDATIONS

1. **For all stakeholders: Recognise the growing vulnerability of consumers in the digital age**
   The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor. It is essential that public and private entities consider this in any process for exercising consumer rights, ideally by working with advocates to understand, refine and track definitions, factors and conditions of vulnerability.

2. **For policy-makers and international organisations: Expand international arrangements to harmonise enforcement approaches**
   Policy-makers must ensure that Data Protection Authorities (DPAs) and other relevant authorities can communicate with each other to address complaints. It is important such agreements create a regulatory arrangement with well-defined processes to oversee its enforcement, favouring hard law and clearly defined collaboration mechanisms that promote clarity and certainty across jurisdictions, instead of depending on self-regulation and ad-hoc, unpredictable coordination.

3. **For policy-makers: Strengthen the options for collective redress**
   Strengthening collective redress mechanisms is essential for addressing widespread data protection issues, as collective actions can better enforce rights for many individuals, compared to rare individual legal actions in this field.

4. **For policy-makers and the private sector: Invest in and experiment with additional informal pathways to conflict resolution**
   Examples include online dispute resolution platforms and data fiduciaries. The existence of informal redress mechanisms should not preclude or replace a consumer's right to access to justice via formal means.

5. **For policy-makers and international organisations: Treat consumers equitably across jurisdictions**
   Develop regulations that support equitable treatment for consumers with different citizenship status, regardless of their nationality or the jurisdiction that is enforcing their rights, when they seek redress for violations arising from international data transfers.

Stakeholders should aim to reflect the highest consumer and data protection standards available, rather than the lowest common denominator.

6. **For international organisations: Continue to pursue regulatory interoperability in the context of a free and open internet**
   Direct efforts towards establishing multilateral and bilateral agreements to facilitate rights-respecting IPDTs, putting consumers' access to redress at the centre of discussions:

   a. Employ a multistakeholder approach (see recommendation 7.) to ensure that interoperability alternatives consider multiple contexts and vulnerabilities;

   b. Respect digital sovereignty and ensure regulations resulting from such agreements consider multiple jurisdictions, and are not simply imposed on low- and middle-income countries by upper-income countries;

   c. Establish transborder regulatory sandboxes in spaces of power such as the OECD and UN, to allow different stakeholders to test and improve the benefits and limits of old and new frameworks of personal data protection;

   d. Where appropriate, provide financial incentives to enable low-income countries to operationalise such agreements.

7. **For international organisations: Consult with civil society and consumer protection bodies**
   In directing efforts towards regulatory interoperability, include a public process of gathering inputs on the local reality of each country, facilitating the creation of regulations that are effective locally and, consequently, globally.

8. **For the private sector: Invest in transparency and the provision of appropriate information to empower consumers in making informed decisions** Enhance consumer awareness about available mechanisms for redress, by providing transparent information that is relevant, timely and inclusive. Such efforts should not preclude appropriate and ongoing investment in data privacy and security to protect consumers.

9. **For regulatory bodies and the private sector: Use technology to facilitate the exercise of rights**
   Invest in technologies that facilitate the exercise of rights, especially in countries where digital literacy is lower. Ensure these technologies have undergone testing and impact assessments prior to being made available for consumer use, and on an ongoing basis. These arrangements should not preclude access to human assistance.

10. **For policy-makers and the private sector: Explore the possibility of a collective fund for redress contributed to by private companies**
    Incentivise private companies to create a fund for redress for consumers. Such a fund, overseen by a multistakeholder board to decide the different cases, should be tasked to ensure that its outcomes are consumer-centred.

1. INTRODUCTION

Cross-border data flows have become essential to the functioning of the global digital economy[1]. They underpin social interactions, international business operations, logistics, supply chains and global communication[2]. This is not just beneficial for consumers in terms of broader access to information and services. Digitally enabled trade, supported by harmonised legal framework built on strong protections for consumer rights and enforceable regulations, can advance inclusive innovation[3], enhance consumer trust through cohesive policies[4], and foster economic growth in emerging markets[5].

But such harmonisation is only as good as its ability to enforce minimum standards of consumer protection, in a manner that adheres to the UN's *Guidelines for Consumer Protection*, and incorporating an approach that leaves jurisdictions enough flexibility to enforce additional layers of protection that consider specific contexts and vulnerabilities.

A large part of data crossing borders is personal data, subject to the more rigorous protection guaranteed by personal data legal frameworks. However, in the context of international personal data transfers (IPDTs), and despite these enhanced protections, there is still significant risk to consumers that their personal data will be misused. Policy-makers in some nations have used this to mandate or justify data localisation, which is the practice of storing and accessing data within the country or region it operated from, and which is regarded as a contributing factor to the 'splintering' of the internet into fragmented networks[6]. While setting this debate aside entirely is difficult, considering that the majority of global data processing taking place in upper-income countries, and with the volume of data being processed only likely to increase in the future, robust redress mechanisms that serve consumers regardless of where in the world they live are a growing priority.

This report reviews and evaluates current options for consumers to seek redress when personal data is misused in the context of IPDTs. The *misuse of personal data* means any non-compliant processing of personal data. Common examples of personal data misuse include *breach* of personal data, *collection error* (ie, an instance in which personal data is incorrectly or unnecessarily collected without a legitimate legal basis) and *unauthorised use* (when personal data is processed for a certain purpose, but is ultimately used by the data controller for another purpose). *Redress* means all available administrative and judicial remedies consumers may access to obtain compensation, or repair or restore a situation of data misuse. It also includes a consumer's rights as a data subject,

---

[1] Organisation for Economic Co-operation and Development. (n.d.) *Data free flow with trust*. https://www.oecd.org/digital/data-free-flow-with-trust/.

[2] Organisation for Economic Co-operation and Development (n.d.). *Cross-border data flows.* https://www.oecd.org/en/topics/cross-border-data-flows.html.

[3] International Monetary Fund (2021) *Toward a Global Approach to Data in the Digital Age.* https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264

[4] Center for Global Development (2021) *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity* https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and

[5] United Nations Conference on Trade and Development (2016) *Data protection regulations and international data flows: Implications for trade and development.* https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

[6] Organisation for Economic Co-operation and Development (2020). Data localisation trends and challenges. *OECD Digital Economy Papers No. 301,* OECD Publishing, Paris

such as rights to access, correction, erasure and objection, data portability, and the right to revoke consent.

This report further provides recommendations to policy-makers, regulators, civil society and industry for strengthening the protection of consumer rights and the overall consumer experience. The protection of consumers' personal data rights is a critical concern in the context of IPDT. The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor[7]. Because IPDTs have become integral to trade expansion and economic growth, it is imperative that the utmost care is taken to protect consumers, so as not to undermine confidence in the global economy.

2. RESEARCH METHODOLOGY

This report reviews lawful mechanisms for IPDT as they are represented in the following five legal frameworks:

1. the European Union's General Data Protection Regulation (GDPR)[8];
2. the Council of Europe's Convention 108+[9];
3. the Asia-Pacific Economic Cooperation (APEC)'s Privacy Framework[10];
4. the Standards for Personal Data Protection for Ibero-American Data Protection Network[11] (RedIPD – acronym in Spanish); and
5. the Brazilian General Data Protection Law (LGPD)[12].

These legal frameworks were selected for review based on availability of information (GDPR, LGPD), current and future global relevance (GDPR, APEC Privacy Framework), regional relevance (RedIPD, APEC Privacy Framework), diversity, (RedIPD, APEC Privacy Framework) and contextual importance (LGPD, since Brazil currently holds the presidency of the G20). Almost all of the legal frameworks selected encompass more than one jurisdiction[13]. In total, 39 jurisdictions are touched by the frameworks reviewed in this report.

[7] Organisation for Economic Co-operation and Development. (2023). Consumer vulnerability in the digital age. *OECD Digital Economy Papers, No. 355*, OECD Publishing, Paris

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[9] Council of Europe. (2018) *Convention 108 + Convention for the protection of individuals with regard to the processing of personal data* https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[10] Asia-Pacific Economic Cooperation (2005) *APEC Privacy Framework* https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

[11] Red-Iberoamericana de Proteccion de Datos (2017) *Standards For Personal Data Protection For Ibero-American States* https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf

[12] Lei Nº 13.709, De 14 De Agosto De 2018, see https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[13] See Annexe 1 for details of jurisdictions covered by the selected frameworks.

The lawful basis for international personal data transfers (referred to in this report as the *IPDT mechanisms*) varies across these legal frameworks. Within the selected frameworks are four varying and sometimes overlapping IPDT mechanisms:

1. adequacy decisions (GDPR);
2. standard contractual clauses (SCCs) (GDPR, RedIPD, LGPD);
3. certification (APEC Privacy Framework); and
4. consent (found across all the legal frameworks we analysed).

Using the United Nations's *Guidelines for Consumer Protection*[14] as a point of reference, we review options for redress for consumers within each of these IPDT mechanisms, in each of the legal frameworks in which they appear. Then, drawing on existing literature, case studies and interviews conducted with stakeholders from different regions and areas of expertise, we unearth challenges to consumer-centric redress, and opportunities for change.

The report finishes with ten recommendations that draw on this research, which aim to strengthen the options available to consumers seeking redress when their personal data is misused in the context of IPDTs.

This report focuses on IPDT mechanisms in which the data being transferred belongs to a consumer, as defined by the United Nations's *Guidelines for Consumer Protection*. The focus on consumers differs from the focus of national data protection frameworks, which are concerned with the personal data rights of individuals, also known as *data subjects.* Thus, this report employs the term *consumer* to refer to an individual, both in relation to their consumer rights, as well as their rights as a data subject.

Finally, this report focuses on the options for redress available within the selected legal frameworks. There are other available avenues for redress, such as the private right of action, collective redress alternatives, and administrative procedures within consumer protection agencies, however these are not explored in this report.

3. IPDT MECHANISMS AND OPTIONS FOR REDRESS

This section analyses the selected IPDT mechanisms and identifies possible ways for consumers to access redress in the event their data is misused.

3.1 ADEQUACY DECISIONS: GDPR AND THE EU-US DATA PRIVACY FRAMEWORK

An adequacy decision occurs when the Data Protection Authority (DPA) of a given country or legislature determines that another country provides an adequate level of data protection for the purposes of IPDT. In July 2023, the European Commission adopted its adequacy decision for the United States in the form of the EU-US Data Privacy Framework (EU-US DPF), replacing the previous Privacy Shield, which had been declared invalid[15]. This decision asserts that the United States has an adequate level of protection for personal data transferred from the EU to US companies and

[14] United Nations (2016) *Guidelines For Consumer Protection* https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf

[15] BBC News (2020) EU-US Privacy Shield for data struck down by court https://www.bbc.co.uk/news/technology-53418898. For more information see: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en.

organisations participating in the EU-US DPF, a programme administered by the International Trade Administration in the US Department of Commerce that enables eligible US-based organisations to self-certify[16] their compliance with various safeguards.

Under the EU-US DPF a consumer has different avenues for redress, depending on who is processing their data and why[17]. This report focuses on the avenues available for consumers to seek redress from commercial organisations (there are separate avenues for redress specified in the framework where data is being misused by US law enforcement or US intelligence agencies).

A consumer seeking redress against a US company participating in the EU-US DPF that has violated its obligations under that framework has several alternatives[18]. They can:

1. Contact the organisation that is participating in the DPF, from the company records available at the DPF website[19]. The organisation must respond within 45 days;
2. Contact the free independent recourse mechanism, designated by the organisation in its programme record;
3. Submit a complaint directly to their national DPA, who will then refer the complaint to the US Department of Commerce's International Trade Administration on behalf of the consumer;
4. Invoke binding arbitration[20], which has specific requirements, including that prior to initiating the arbitration claim, the consumer has to have used all the other alternatives listed above. The arbitral tribunal only has authority over individual cases, and it can impose specific individual, non-monetary equitable relief (such as access to data, correction, deletion or return of the individual's data) to remedy the violation[21];

[16] Data Privacy Framework Program (n.d.) *6–Self Certification* https://www.dataprivacyframework.gov/framework-article/6%E2%80%93Self-Certification

[17] Hogan Lovells (2024) *Data Privacy Framework: Redress mechanisms for EU individuals get a boost with new EDPB resources.* https://www.engage.hoganlovells.com/knowledgeservices/news/data-privacy-framework-redress-mechanisms-for-eu-individuals-get-a-boost-with-new-edpb-resources

[18] Data Privacy Framework Program (n.d.) *How to Submit a Complaint Relating to a Participating Organization's Compliance with the DPF Principles* https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization%E2%80%99s-Compliance-with-the-DPF-Principles

[19] Data Privacy Framework Program (n.d.) *Data Privacy Framework List* https://www.dataprivacyframework.gov/list

[20] International Centre for Dispute Resolution American Arbitration Association (n.d.) *The EU-U.S. DPF and UK Extension to the EU-U.S. DPF Annex I Binding Arbitration Mechanism* https://go.adr.org/dpfeufiling.html

[21] *ibid.*

5. Contact the relevant US enforcement authority, which is in each organisation's DPF programme record, and in most instances is the Federal Trade Commission (FTC)[22]. The FTC does not mediate individual complaints–it uses its database of complaints to guide it in initiating its own investigations.

CASE STUDY: CAMBRIDGE ANALYTICA

In 2015, reports emerged[1] about Cambridge Analytica, a UK-based data mining company, which harvested Facebook user data to influence political campaigns, leveraging data collected from an app on Facebook to create psychometric algorithms predicting political preferences. The scandal gained prominence, with accusations that the company manipulated the 2016 US elections and the Brexit referendum[1].

Regulatory responses focused on the misuse of Facebook data, leading to fines and legal actions. For instance, the UK Information Commissioner's Office (ICO) fined Facebook £500,000, while the US Federal Trade Commission (FTC) imposed a $5 billion fine[1], besides also finding[1] that Cambridge Analytica had failed to adhere to the principles of Privacy Shield or to renew its certification.

The scandal spurred regulatory changes globally, such as the EU's Digital Services Act, aimed at addressing social media manipulation and data privacy concerns.

The data protection case against Cambridge Analytica was triggered by its failure to respond to a subject access request by a US citizen, Professor David Carroll[1]. Carroll filed a suit at the High Court in London, requiring Cambridge Analytica to hand over all the data they had on him. Due to the scandal following the publication of Cambridge Analytica's wrongdoings, the company filed for bankruptcy, halting the progress of the data protection case. Although Carroll continued with his demand through the bankruptcy case, he lost and had to pay a significant adverse cost, which in his case was paid with money raised through crowdfunding[1]. What this case shows regarding redress is how redress for data misuse is hard for individuals: Carroll accessed a court outside of his home country, had to pay for the lawsuit, and ended up having to pay adverse costs.

3.2 STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (SCCs) are standardised and pre-approved model data protection clauses that allow data controllers and data processors to comply with their obligations under a certain personal data protection framework. They appear across several of the legal frameworks that are the focus of this study. SCCs are validated by a country authority and signed between the entity transferring personal data (the *data exporter*) and the entity receiving it (the *data importer*). The clauses are designed to ensure that IPDTs occur under appropriate safeguards,

[22] Data Privacy Framework Program (n.d.) *How to Submit a Complaint Relating to a Participating Organization's Compliance with the DPF Principles* https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization%E2%80%99s-Compliance-with-the-DPF-Principles

including the availability of effective legal remedy in the event of misuse of personal data (enshrined in Art. 46.1 of GDPR and art. 33, II of LGPD).

3.2.1 STANDARD CONTRACTUAL CLAUSES IN GDPR

The GDPR allows for the transfer of personal data to a "third country" (ie a country outside the European Economic Area (EEA)) in the absence of an adequacy decision, as long as the data exporter: (1) has provided appropriate safeguards, and (2) there are enforceable data subject rights and effective legal remedies for data subjects are available in that third country. One of the manners of ensuring both of these requirements is to apply standard data protection clauses (drafted by the European Commission) in the commercial agreement. Given the current scenario in which not all countries have broad adequacy decisions regarding GDPR data protection levels, within the GDPR, these SCCs are an important IPDT mechanism.

The SCCs for IPDTs contain specific data protection safeguards to ensure that personal data continues to enjoy a high level of protection when internationally transferred[23]. The SCCs safeguard individual rights to information about the transfer of the data outside of the EEA[24] and the right to obtain a copy of the clauses on request, free of charge[25].

In this set up, a consumer seeking redress when their data has been processed in violation of the SCCs has several alternatives[26]. They can:

1. Lodge a complaint with the data importer through a designated contact point. The data importer may further offer the option to lodge a complaint through a designated independent dispute resolution body.
2. Lodge a complaint with the DPA of the EEA country where the consumer lives, against either the data importer or exporter.
3. Initiate court proceedings for injunctive relief or compensation in the EEA country where they live, or as designated by the parties to the SCCs.

Additionally, consumers can seek redress under the GDPR against the data exporter by complaining within the EU to a national DPA and/or obtaining judicial remedy, depending on the national legal framework.

[23] European Commission (n.d.) *New Standard Contractual Clauses - Questions and Answers overview* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions

[24] *ibid.*

[25] *ibid.*

[26] *ibid.*

CASE STUDY: CASE C-311/18 (SCHREMS II)

In 2020, the Court of Justice of the European Union (CJEU) invalidated the partial EU-US adequacy and certification regime called Privacy Shield in the Schrems II case[1]. The Court found that Privacy Shield did not adequately protect EU citizens from US mass surveillance and lacked enforceable rights for redress. Following the ruling, many companies switched to alternative mechanisms like SCCs or consent, but smaller entities faced uncertainty until the new EU-US Data Privacy Framework (DPF) was implemented.

Beyond Privacy Shield's invalidation, the Schrems II decision also cast doubt over the use of SCCs. The CJEU ruled that SCCs could be valid, but only if effective mechanisms and protections existed in the destination country, which it had ruled was not the case in the US.

The CJEU decision obliged organisations using SCCs to be certain that the legal environment in the destination country of data transfer allowed the effective execution of the clauses, through conducting Transfer Impact Assessments (TIAs) and implementing additional safeguards where necessary. The European Commission updated the SCCs[1], and the European Data Protection Board provided recommendations[1] to help data exporters navigate these requirements. Similar measures have been adopted in the UK[1] and Canada[1] to address cross-border data transfer challenges.

Max Schrems, the Austrian privacy activist and lawyer involved with the case was interviewed for this project.

3.2.2 STANDARD CONTRACTUAL CLAUSES IN LGPD

Despite being inspired by the GDPR, LGPD is a source of data protection that sits apart from the Global North axis, with a DPA (known in Brazil as the National Data Protection Authority, or ANPD) that is committed to regulating international data transfers. ANPD is in the process of creating detailed rules for international transfers, having already published a first resolution of these rules[27], which establishes procedures for adequacy decisions and contractual mechanisms for carrying out IPDT, including a model for SCCs.

The resolution contains transparency obligations in respect of the data controller, to make SCCs available to the consumer on request[28]. The controller must publish the rights of the consumer and the means to exercise those rights, including a channel to communicate with the controller and the right to make a complaint before the DPA[29].

A consumer seeking redress when their data has been processed in violation of the SCCs has several alternatives. They can:

[27] Gov.br (2024) Resolução Cd/ANPD Nº 19, De 23 De Agosto De 2024 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396

[28] *ibid.*

[29] *ibid.*

1. Assert their rights individually and collectively, using existing legislation in Brazil[30];
2. File lawsuits against the data exporter or the data importer, in Brazilian courts;
3. Seek arbitration between the parties to resolve disputes, as long as the arbitration is done in Brazil and according to Brazilian arbitration law[31].

3.2.3 STANDARD CONTRACTUAL CLAUSES OF THE IBERO-AMERICAN DATA PROTECTION NETWORK

The Ibero-American Data Protection Network (RedIPD) is a forum that brings together public and private stakeholders (including 22 data protection authorities) from Spain, Portugal, Mexico, and other countries in Central and South America and the Caribbean. RedIPD's mission is to foster information exchange and promote regulatory developments for advanced personal data protection.

In 2017 RedIPD published its *Standards for Personal Data Protection for Ibero-American States*[32]. One explicit aim of this set of standards was to make the flow of personal data between RedIPD states easier, in order to enable economic and social growth in the region and foster international cooperation. These standards define the IPDT mechanisms available in this framework, which include SCCs.

In February 2023, RedIPD released a set of SCCs[33] and a guide[34] for their implementation. The SCCs include a specific clause related to redress. It states that the data importer must provide consumers with a contact point for complaints in a transparent and easily accessible format. Data importers can further provide consumers the option to lodge a complaint with an independent dispute resolution body free of charge, but they must not oblige consumers to follow a particular sequence in seeking redress.

The SCCs further state that data exporters and data importers who receive complaints from consumers should make every effort to resolve the matter "amicably and in a timely fashion", collaborating, where appropriate, "in good faith".[35] The SCCs go on to specify that the data controllers involved in the IPDT will not dispute a consumer's decision to file a complaint with the DPA of their country of residence or workplace, nor will they challenge a consumer's right to bring legal proceedings. Consumers can bring legal proceedings against the data exporter and/or the data importer in the country of the data exporter or in the country in which the consumer has his/her habitual residence, and they can bring legal proceedings against the data importer in the country of the data importer.

[30] *ibid.*

[31] *ibid*.

[32] Red-Iberoamericana de Proteccion de Datos (2017) *Standards For Personal Data Protection For Ibero-American States* https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf.

[33] Red-Iberoamericana de Proteccion de Datos (2023a) *Annex: Model Contractual Clauses* https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf

[34] Red-Iberoamericana de Proteccion de Datos (2023b) *Implementation Guide: On Model Contractual Clauses for International Personal Data Transfers (IPDT)* https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-en.pdf

[35] Red-Iberoamericana de Proteccion de Datos (2023a) *Annex: Model Contractual Clauses* https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf

3.3 APEC's Certification System

Certification is a formal process where an organisation is evaluated and approved to engage in IPDTs. Asia-Pacific Economic Cooperation (APEC)'s Cross Border Privacy Rules (CBPR) certification system was designed by APEC to create a framework of trust in personal data cross-border flows, based on the APEC Privacy Framework. One of its explicit aims is to foster trust between consumers, businesses, and regulators when it comes to IPDTs.

APEC's CBPR is a growing arrangement, an open agreement to which other countries can join. Members of its Joint Oversight Panel are encouraged to seek other participants. In this sense, it appears to aspire to becoming a global standard. Currently, nine countries are part of the APEC CBPR system (USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines)[36], with more expected to join soon.

APEC's Privacy Framework features nine principles: accountability, prevention of harm, notice, choice, collection limitation, use of personal information, integrity of personal information, security safeguard, and access and correction. The APEC privacy rules were inspired by the OECD Privacy Guidelines[37], considered a "minimum standard…for the protection of privacy and individual liberties"[38].

Businesses participating in the APEC CBPR System are required to adopt data privacy practices and structures that align with the APEC Privacy Framework. These practices and structures are evaluated for compliance by an accountability agent (an independent entity recognised by the APEC CBPR system). The system is administered by the Joint Oversight Panel, which provides oversight to accountability agents, resolves conflicts of interest; and manages complaints.

A directory of CBPR-certified organisations is maintained at https://cbprs.org/. Under this system, a consumer seeking redress for data misuse is initially directed to resolve the issue directly with the CBPR-certified organisation. If the outcome is unsatisfactory, they can:

1. file a complaint about a CBPR-certified organisation to the accountability agent that certified the organisation;
2. file a complaint to the relevant privacy enforcement authority listed in the compliance directory;
3. Send an email to an address administered by the US International Trade Administration. If an organisation claims to be a CBPR System participant but is not listed in the compliance directory, the consumer can also report this to the same email address.

To ensure enforcement, a Cooperation Arrangement[39] outlines a practical multilateral mechanism for Privacy Enforcement Authorities to collaborate on cross-border privacy enforcement.

---

[36] US Department of Commerce (n.d.) *Global Cross-Border Privacy Rules Declaration* https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[37] Organisation for Economic Co-operation and Development (2001) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf

[38] *ibid.*

[39] Asia-Pacific Economic Cooperation (n.d.) APEC Cooperation Arrangement For Cross-Border Privacy Enforcement https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

It provides a framework for Privacy Enforcement Authorities to voluntarily share information, request assistance, and render aid in specific ways.

3.4 CONSENT

Consent is a legitimate basis for national personal data processing in almost all personal data protection frameworks worldwide, as well as an IPDT mechanism in some of them, such as GDPR[40], LGPD[41] and the Council of Europe's Convention 108+[42].

Considering common bases of each of the frameworks that provide for consent as an IPDT mechanism, consent must be, at a minimum, informed, explicit, specific and freely given, being limited to the purpose of the international transfer. This greater qualification of consent creates obligations for the controller. First, to obtain valid consent, the consumer must give an express statement agreeing to the processing of their personal data for the specific purpose of the international transfer, ideally through granular alternatives. Second, the consumer must be adequately informed about the international transfer and its purpose, which means the use of clear and plain language that would be understood by the average person[43]. Finally, the consumer must be able to freely agree with the international transfer, without any form of coercion, being able to withhold consent and eventually revoke it[44]. In situations where there is an imbalance of power, consent may not be a suitable legal basis for processing, as it may not be considered to have been given freely[45].

As consent is presented in different personal data protection frameworks, its management varies according to the jurisdiction and region, and depending on the platform or marketplace being used. As such, the available redress options will also depend on the possibilities available both in the applied legal framework and in national legislation. This may lead to different levels of protection and lack of consistent approaches[46]. A global consumer study conducted by Visa found that 62% of consumers prefer companies to offer standardised, simple explanations when seeking consent[47].

[40] General Data Protection Regulation (EU) 2016/679, art 49, available at https://eur-lex.europa.eu/eli/reg/2016/679

[41] Brazilian General Data Protection Law (LGPD), art 5, XII, available at https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

[42] Council of Europe Convention 108+, art 14 (4), available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[43] European Data Protection Board (2020). *Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[44] Frajhof, Isabella Z.; Sombra, Thiago Luís. (2020) A transferência internacional de dados pessoais. In: Mulholland, Caitlin. A *LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélogo, pp. 265-288

[45] Marelli, Massimo. (2024) Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms. *International Data Privacy Law*, Vol. 14, No. 1.

[46] Visa (n.d.) *Consent Management Guidelines.* https://globalclient.visa.com/ConsentManagement

[47] Visa (2024) *Consumer Empowerment Study.* https://globalclient.visa.com/ConsentManagement

CASE STUDY: THE US SUPREME COURT

The US Supreme Court's handling of data protection cases poses challenges for cross-border data governance, especially for redress mechanisms and interoperability. In the 2021 TransUnion LLC v. Ramirez case[1], the Court restricted standing for plaintiffs to those who could prove "concrete" harm from a defendant's statutory violation. Where TransUnion falsely labelled 8,185 individuals as potential terrorists, the Court found only 1,853 had standing, due to dissemination of their credit reports to third-party business.

This ruling has been criticised for making it difficult to address privacy violations that don't result in immediate, tangible harm. Legal scholars argue that privacy harms can be hard to quantify, and the requirement for concrete injury leaves many violations unaddressed. The decision reflects a broader trend in US courts, where proving harm is challenging, particularly in data breach cases[1].

US rulings are especially relevant when considering redress mechanisms, because a considerable amount of companies processing personal data involved in IPDTs are under US jurisdiction. This restriction on privacy violations, therefore, affects consumers beyond US borders, should they try to use US jurisdiction to obtain redress.

4. ANALYSIS AGAINST UN *GUIDELINES FOR CONSUMER PROTECTION* OF OPTIONS FOR REDRESS IN IPDT MECHANISMS

Consumer protection and empowerment is critical to making markets work well for trade, business and governments, as well as for consumers themselves[48]. Since 1985, the United Nations has maintained a set of *Guidelines for Consumer Protection*[49], principles designed to ensure effective consumer protection legislation, enforcement institutions, and redress systems. These guidelines aim to assist member states in formulating and enforcing domestic and regional laws, rules, and regulations.

The UN guidelines stipulate that consumers using electronic commerce should receive the same level of protection as in other forms of commerce[50]. They assert the need to safeguard consumer privacy while also supporting the global free flow of information[51].

---

[48] Consumers International (n.d.) *What We Do: Our Consumer Protection and Empowerment Index: a Unique Tool to Guide Marketplace Change.* https://www.consumersinternational.org/what-we-do/the-global-index/.

[49] United Nations (2016) *Guidelines For Consumer Protection* https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf

[50] *ibid*, General Principles, 5j

[51] *ibid*, General Principles, 5k

The UN guidelines emphasise effective dispute resolution and redress. According to the guidelines, member states should encourage:

> *…fair, effective, transparent and impartial mechanisms to address consumer complaints through administrative, judicial and alternative dispute resolution, including for cross-border cases."*[52]

They should ensure legal and/or administrative measures to enable consumers or their relevant representative organisations to obtain redress. The principles specify that this can be achieved through formal or informal procedures, but that in either case such measures must be "expeditious, fair, transparent, inexpensive and accessible"[53] and must consider the special needs of vulnerable and disadvantaged consumers. Of particular relevance to this research, the guidelines specify that access to redress measures should be enhanced in the case of cross-border disputes. The UN guidelines reaffirm the need for collective resolution procedures that must follow the same qualifications of being expeditious, transparent, fair, inexpensive and accessible.

Finally, the UN guidelines encourage businesses to provide accessible, fair, transparent, affordable, and efficient mechanisms for resolving complaints promptly and effectively when things go wrong. They recommend that businesses adhere to local and global standards for internal complaint handling, alternative dispute resolution, and customer satisfaction codes.

In summary, to satisfy the UN guidelines, redress mechanisms for data misuse in the context of IPDTs should be:

- fair, effective, and impartial;
- accessed through formal or informal procedures;
- able to accommodate collective action;
- inexpensive, efficient and timely;
- transparent and accessible; and
- considerate of the special needs of vulnerable and disadvantaged consumers

We now analyse each of the IPDT redress mechanisms against the above criteria.

4.1 ADEQUACY DECISIONS: GDPR AND THE EU-US DATA PRIVACY FRAMEWORK (DPF)

Within the EU-US DPF, if an organisation is not fulfilling its obligations under the framework principles, a consumer has different options. They can contact the organisation directly, use a free independent recourse mechanism designated by the organisation, submit a complaint to their national DPA, invoke binding arbitration, or contact the relevant US enforcement authority.

Each of these options has its pitfalls. First, the consumer has to be aware which organisation is responsible for the misuse of their data. Second, contacting the organisation directly can yield no results, and if that is the case, before they can invoke binding arbitration, the consumer has to try the free independent recourse mechanism, and also submit a complaint to their DPA. If the consumer gets as far as binding arbitration, the results are limited, since only non-monetary equitable relief is available (eg access to data, correction or deletion). Only individuals can complain, and remedy is also on an individual basis (ie there is no possibility of collective action.) Lastly, if the

[52] *ibid.*

[53] *ibid.*

consumer decides to contact the US enforcement authority, which will almost always be the FTC, it does not solve individual complaints.

Thus there is potentially a long path that the consumer has to follow to have their complaint solved, a path that further demands initial knowledge that might not be accessible, that can have limited results, and that is only applicable to the individual. We should note that the DPF website does give information on the forms of redress available, as well as relevant contact points with whom to initiate complaints.

4.2 STANDARD CONTRACTUAL CLAUSES (SCCS)

Within the context of the SCCs provided for in the GDPR framework, consumers may seek redress for data misuse by initiating court proceedings or proceedings at an independent dispute resolution body, or they may lodge a complaint with the data importer, or the DPA either of the country in which they reside or of the country where the data exporter is based. The consumer also has information rights: the right to be informed about the transfer of the data outside of the EEA, and the right to obtain a copy of the clauses, free of charge, on request[54]. Comparing these options for redress against the UN *Guidelines for Consumer Protection*, it is possible to state only that there are redress mechanisms accessed by both formal and informal procedures, and that there is a transparency obligation (ie the right of information for consumers) There is not sufficient information to evaluate options for redress within this framework against the other criteria of the UN guidelines.

In LGPD's SCCs, the data subject has several rights that are enforceable against the agents processing data in IPDT (ie. the data exporter and data importer), including information rights. Specifically concerning redress, there is authorisation for claims to be filed by consumers either individually or collectively, against the exporter or the importer, in Brazilian courts. There is also authorisation for the use of arbitration between the parties to resolve disputes, as long as the arbitration is done in Brazil and according to the Brazilian arbitration law. As with SCCs in the GDPR framework, comparing this mechanism against the UN *Guidelines for Consumer Protection*, it is possible to state that there are redress mechanisms with formal and informal procedures and a transparency obligation (the right of information for consumers). Additionally, this system is able to accommodate collective action.

Red-IPD SCCs create an obligation for the data importer to provide consumers with a contact point for complaints in a transparent and easily accessible format. This meets the transparency requirement of the UN *Guidelines for Consumer Protection*. In Red-IPD's model, data subjects have the right to redress through a free, simple and timely procedure, in line with the UN guidelines' requirement for inexpensive, efficient and timely redress procedures that include informal options. This requirement is further met by the fact that the Red-IPD model suggests the data importer provides consumers with the option to lodge a complaint, at no cost, with an independent dispute resolution body. Furthermore, the consumer has the right to submit a claim before either the DPA or the relevant court with an obligation on the IPDT agents to try to resolve it amicably and promptly. However, a major concern regarding SCCs is their lack of enforceability, as they are soft law. This means their implementation, supervision, and enforcement depend on the local authorities of each country, making it difficult to ensure a consistent level of protection, given that some countries have more stringent national personal data protection rules than others. It is unclear neither how the

[54] European Commission (n.d.) *New Standard Contractual Clauses - Questions and Answers overview* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions

SCCs will be applied and supervised by the agents nor how consumers will exercise their right to redress in case of personal data misuse.

4.3 CERTIFICATION: APEC'S CROSS BORDER PRIVACY RULES (CBPR)

The APEC certification model presents two clear steps for consumers seeking redress, which is aligned with UN guidelines: consumers are encouraged to resolve their problems directly with the accountability agent who originally certified the organisation; if this fails to address the situation, consumers can contact the Joint Oversight Panel. These two mechanisms do not impose a cost for the consumer. Further, the fact that accountability agents can receive consumer complaints may facilitate the conflict resolution process. However, because of the private character of the APEC framework, these mechanisms are not particularly transparent, including with regard to fairness and timeliness[55]. A practical analysis of these aspects of the APEC redress system could be an important topic for future study.

What makes APEC an interesting framework from a consumer perspective is the Cooperation Arrangement[56] between different national authorities that enables the necessary communication to ensure enforcement across borders. The stipulation that private agents be certified using a common set of requirements overseen by a supranational organisation (the Joint Oversight Panel) presents further opportunities for harmonisation.

The APEC privacy framework needs to be updated in line with current data privacy laws that are more protective of consumers. Furthermore, it is unclear how accountability agents forward consumer complaints, which can create uncertainties in the process. Another disadvantage is that a significant part of the system is led by private parties, who may have an interest in making data processing viable, as this brings profit to certified companies.

4.4 CONSENT

In terms of consent as an IPDT mechanism, it is clear that when adequately obtained, it can foster consumer trust in an organisation, and allow consumers greater control, since consent allows for the consumer to exercise the right to revoke consent. However, the ability to revoke consent at any time renders consent a fragile IPDT mechanism, besides the difficulty it presents to data controllers in ensuring that consent's requirements are all adequately implemented. This makes it hard to comply with the UN guidelines, which include guidance related to cost and complexity for companies.

As noted above, since consent is presented in different personal data protection frameworks, its management varies according to the jurisdiction, region and depending on the platform or marketplace being used. This may lead to different levels of protection and a lack of consistent approaches[57]. This variation on how to manage consent in the global regulatory landscape

[55] Sullivan, C (2019) EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era, *Computer Law & Security Review*, 35 (4), pp 380-397

[56] Asia-Pacific Economic Cooperation (n.d.) APEC Cooperation Arrangement For Cross-Border Privacy Enforcement https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

[57] Visa (n.d.). *Consent Management Guidelines.* https://globalclient.visa.com/ConsentManagement

may create barriers in data flows, as it makes IPDTs more difficult while decreasing consumer trust[58]. It is not possible to evaluate consent per se against the UN *Guidelines for Consumer Protection*, as the available redress options will depend on the possibilities available both in the applied legal framework and in national legislation.There is not enough empirical data regarding international transfers to compare against the UN criteria.

Despite being an IPDT mechanism that empowers the consumer when well implemented, for controlling organisations it can represent a fragile mechanism, since the consumer can, at any time, revoke consent. When this happens, the data controller must immediately stop processing the consumer's personal data, represented by the international transfer, unless it has another IPDT mechanism available.

Additionally, the consent requirements create a series of obligations for the controller which lead to a lack of effectiveness of consent as a safeguard for the valid processing of personal data[59]: when consent was broadly used as the legal basis for personal data processing in the EU, consumers faced an overload of consent requests through pop-up screens or similar instruments, resulting in fatigue on part of the consumers, who chose not to read the various requests, accepting them only so that they can obtain the desired service in a shorter time[60].

Moreover, it is important to note that under the GDPR, consent as an IPDT mechanism is included among the derogations for specific situations in art. 49. According to the interpretation of the former Article 29 Working Party, now the European Data Protection Board (EDPB), the best practice for these situations is to use a layered approach. This means that derogations, including consent, may be used as exceptional residual situations only when there is no adequacy decision nor a way to ensure the same level of protection through SCCs or global corporate rules. Data controllers must also ensure that appropriate safeguards have been put in place and that data subjects enjoy enforceable and effective rights in order to continue benefiting from their fundamental rights and protections in EU law[61].

Thus, derogations should be interpreted restrictively because, as they do not provide adequate protection or appropriate safeguards and transfers based on derogations do not require any prior authorisation from a DPA, transferring personal data to third countries based on derogations leads to increased risks for the rights and freedoms of the data subjects involved. Therefore, the EDPB also recommends that to assess consent as an IPDT mechanism, it is advisable for the data exporter to conduct a necessity test, which requires an evaluation to determine whether an IPDT is necessary for the specific purpose of the derogation being used[62].

Thus, as the selected personal data protection frameworks establish a stringent standard for using consent, especially in GDPR as a derogation, this high threshold, coupled with the fact that a

---

[58] Visa Consumer Empowerment Research (n.d.) *The Role of Consumer Consent and Regulatory Interoperability in Building a Trusted Digital Economy* https://images.globalclient.visa.com/Web/InovantElqVisaCheckout/%7B6e2ee1cf-1605-4044-a6ce-cee57e5053a3%7D_Visa_The_Role_of_Consumer_Consent_and_Regulatory_Interoperability.pdf.

[59] Custers, Bart; Schermer, Bart Willem; Van Der Hof, Simone (2014). *The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection*. Leiden University Faculty of Law, Ethics & Information Technology

[60] Article 29 Data Protection Working Party (2017). *Guidelines on consent under Regulation 2016/679* https://ec.europa.eu/newsroom/article29/redirection/document/51030

[61] European Data Protection Board (2018) *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

[62] *ibid.*

consumer can withdraw their consent at any time, suggests that consent may not be a viable long-term solution for IPDT[63].

5. DISCUSSION

5.1 CHALLENGES FOR CONSUMERS AND BUSINESSES

It is important to note that the options for redress analysed in this report are relatively newly-established. Redress is generally achieved in the context of the available national and regional legal frameworks, with each IPDT mechanism encompassing a plurality of countries. As systems develop, it is essential to ensure that these mechanisms are interoperable, and to prioritise protecting consumers, including a consumer's ability to access redress in line with the UN's *Guidelines for Consumer Protection.*

Existing redress mechanisms are complex and often inadequate for international consumer grievances[64]. Jurisdictional barriers and varying legal protections hinder the enforcement of consumer rights in cross-border data issues[65]. Challenges to litigation include inconsistencies in enforcement across jurisdictions, varying appeal fees (which affects accessibility), and regulatory ineffectiveness. Some DPAs, like the Irish DPA, are criticised for inadequate action on complaints[66]. Large fines, resulting from lawsuits over personal data misuse, such as the €1.2 billion fine against Meta[67] issued by the EDPB, often face delays or are not fully enforced. Penalties frequently do not reflect the financial benefits of non-compliance for companies[68]. Additionally, non-EU citizens face difficulties seeking redress in EU jurisdictions, with potential disparities in access to justice[69].

From the corporate perspective, managing data flow across borders is challenging due to the lack of global standards. This is true for global businesses[70], and also for SMEs. Globalising SMEs face challenges with fragmented data protection regulations, leading to higher compliance costs and uncertainties[71]. Regional frameworks help, but face implementation challenges. There's a need for better regional mechanisms to aid SMEs and harmonise regulations[72].

---

[63] *ibid.*

[64] Romain Perray, interview conducted for this research, July 30, 2024

[65] *ibid.*

[66] Max Schrems, interview conducted for this research, July 18, 2024

[67] European Data Protection Board (2023) *1.2 billion euro fine for Facebook as a result of EDPB binding decision* https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

[68] Max Schrems, interview conducted for this research, July 18, 2024

[69] Romain Perray, interview conducted for this research, July 30, 2024

[70] Juliana Mozachi Sandri, interview conducted for this research, August 7, 2024

[71] Kati Suominen, interview conducted for this research, August 2, 2024

[72] *ibid.*

5.2 IMPROVING EXISTING SYSTEMS

5.2.1 THE USE OF TECHNOLOGIES IN EDUCATION AND AWARENESS-RAISING

Technology can play a valuable role in upholding and strengthening consumer protection, and in enhancing consumer empowerment. The use of enforcement technology (EnfTech) in consumer law is recognised[73], while leveraging technology to enhance international redress mechanisms, for example through expanding online dispute resolution (ODR) initiatives, can play a role in improving the situation for consumers[74]. A Visa Consumer Study found that 60% of global consumers have not had an opportunity to take any courses teaching them about how to protect their data online[75]. Data exporters and importers should work to enhance consumer awareness by providing transparent information[76] that is relevant, timely and inclusive, and to educate consumers about how to access redress in the consumer's country, and the structures behind exercising the right to redress.

It is important that private and public entities invest in technologies that facilitate the exercise of rights, especially in countries where digital literacy is lower[77]. This could be software that helps consumers draft complaints, or provides templates for situations described by them at the beginning of their interaction with an organisation. The Massachusetts Institute of Technology Future of Data Initiative has recently partnered with industry to develop a Traceability Protocol (OTrace)[78] that aims to harmonise frameworks between organisations, to provide visibility into data flows for consumers. For personal data controllers and processors, it is essential that technologies used to support compliance have undergone testing and impact assessments prior to being made available for consumer use, and on an ongoing basis. These arrangements should not preclude access to human assistance, such as giving consumers the ability to consult with independent legal advisors at no cost, to review a complaint before going to court.

5.2.2 INFORMAL PATHWAYS TO REDRESS

Policy-makers should work to develop and enhance informal mechanisms for seeking redress. A good example of this is the Brazilian website consumidor.gov.br, which has proven to be an effective government platform for consumer redress. It links companies and consumers, giving them the opportunity to resolve a problem in a fast and costless way. In APEC's arrangement, consumers can contact the Joint Oversight Panel, which also has the function of complaint handling; one way to expand this would be to have in-person and online alternatives of dispute resolution through conflict resolution and mediation channels, such as those made available on consumidor.gov.br.

---

[73] Reifa, C and Coll, L (2024) *The transformative potential of Enforcement Technology (EnfTech) in consumer law* https://static1.squarespace.com/static/638646cea1515c69b8f572cb/t/65a522dbeafaaf1208982746/1705321180457/EnfTech_final+report_2024.pdf

[74] *ibid.*

[75] Visa (2024) *Consumer Empowerment Study.* https://globalclient.visa.com/ConsentManagement

[76] Consumers International (2024) *Transparent Digital Finance for Consumers.* https://www.consumersinternational.org/media/534803/transparent-digital-finance-for-consumers.pdf

[77] UNESCO (2018) *Guidelines for Designing Inclusive Digital Solutions and Developing Digital Skills* https://www.unesco.org/en/articles/unesco-launches-guidelines-inclusive-digital-solutions-people-low-skills-and-low-literacy

[78] MIT (n.d.) *MIT Future of Data Initiative.* https://futureofdata.mit.edu/

The creation of informal dispute resolution spaces can also be initiated by private actors. The website reclameaqui.com.br (which translates as "complain here") is a research, reputation and trust platform created for consumers and companies to resolve conflicts. It allows consumers to assign specific companies a rating, which can encourage better practices. Consumers can also disclose cases where they were unable to obtain redress for the misuse of their personal data in IPDT.

Expanding the concept of data fiduciaries (defined as broadly experimental organisations and technologies that act on behalf of data subjects to provide fiduciary stewardship of their data[79]) might better protect data rights, particularly in less developed regions. While some jurisdictions recognise data fiduciaries, this role is not widespread, particularly in the Global South. Expanding this role could help address the needs of consumers in these regions[80].

Another alternative pathway for redress could be to incentivise private companies and global organisations to create a fund for redress for consumers. Such a fund, overseen by a multistakeholder board to decide the different cases, should be tasked to ensure that its outcomes are consumer-centred. This alternative could also prove attractive to the companies, who will have less uncertainty than when faced with a lawsuit or administrative proceeding[81].

Where established, any such informal mechanisms for consumer redress must follow a set of principles that ensure consumers' interests as a priority. And it is essential that the existence of informal redress mechanisms does not preclude or replace a consumer's right to access to justice via formal means. Rather, these mechanisms should be additional layers to enable consumers to seek redress before going to court, a process that can take more time and also be more expensive.

5.2.3 FORMAL PATHWAYS TO REDRESS

Policy-makers must ensure that DPAs and other relevant authorities can communicate with each other to address complaints. It is important such agreements create a regulatory arrangement with well-defined processes to oversee its enforcement, favouring hard law initiatives instead of depending on self-regulation. Without a formal arrangement, such as the one evident in the APEC system, authorities of different jurisdictions are not bound to cooperate, but rather left to do so voluntarily.

5.2.4 COLLECTIVE ACTION

Ensuring legal standing for civil society organisations and public bodies to bring claims to court representing consumers in collective actions could constitute an important step towards meaningful enforcement. Damage caused by IPDTs typically affects a group of people, and the costs of access to justice tend to be high. In the area of data protection, evidence indicates differences between countries in terms of the available mechanisms, the professionals involved, and their experience in dealing with redress[82]. Strengthening collective redress mechanisms is essential for addressing widespread data protection issues, as collective actions can better enforce rights for

[79] van Geuns, J and Brandusescu, A (2020) Shifting Power Through Data Governance Mozilla Insights https://assets.mofoprod.net/network/documents/ShiftingPower.pdf

[80] Lorrayne Porciuncula, interview conducted for this research, August 9, 2024

[81] Lorrayne Porciuncula, interview conducted for this research, August 9, 2024; Kati Suominen, interview conducted for this research, August 2, 2024

[82] European Agency for Fundamental Rights (2014) *Access to data protection remedies in EU Member States* https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

many individuals, compared to rare individual legal actions in this field[83]. Civil litigation and class actions can be effective alternatives for addressing large-scale data breaches[84].

Structuring collective redress mechanisms could mean, for example, creating incentives for courts to prioritise the judgements of strategic collective actions. Where there are already options for collective action, they should be reviewed to ensure that there is enough incentive for consumers to use them, for example the availability of legal aid or whether losing parties are required to pay adverse costs. Collective mechanisms should also be applicable in the context of SCCs: consumers should be able to be represented by third parties and to discuss clauses that impact them collectivity and not just as individuals[85].

5.3 THE FRONTIER OF REGULATORY INTEROPERABILITY

Consumer efforts to seek redress in the case of misuse of personal data in IPDTs are hampered by the fact that redress mechanisms are generally underpinned by the actions of multiple national authorities and in the context of different personal data frameworks. In this scenario, regulatory interoperability may play a crucial role.

Simply put, regulatory interoperability is the ability of different regulatory systems to connect. It is not a binary, but a process, achieved through the coming together of operating rules, business incentives and technical integration[86]. In privacy and data protection regimes, this capacity to work together may facilitate IPDTs, enabling a common protection regime between various jurisdictions. Interoperability does not require these systems to be identical, but rather to converge towards the same underlying principles[87]. Such a convergence could help consumers more easily obtain redress in the case of personal data misuse in IPDTs.

Besides benefiting consumers seeking redress, common rules and principles across different legal systems could help lower transaction costs, reduce barriers to international trade, and promote intangible benefits, such as the safeguarding of fundamental rights[88]. Yet to meet the needs of consumers, it is essential that any attempt to achieve compatibility or harmonisation between different regulations does not lead to a lowering of protection standards or a reduction in safeguards and regulatory requirements overall. In other words, instead of lowering standards to meet the

[83] Max Schrems, interview conducted for this research, July 18, 2024

[84] *ibid.*

[85] Romain Perray, interview conducted for this research, July 30, 2024

[86] Garcia Arabehety, Pablo, Gregory Chen, William Cook, and Claudia McKay (2016) Digital Finance Interoperability

& Financial Inclusion: A 20-Country Scan. Working Paper. Washington, D.C.: CGAP.

[87] Robinson, Lisa; Kizawa, Kosuke; Ronchi, Elettra. *Interoperability of privacy and data protection frameworks. Going Digital Toolkit Note* http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf.

[88] Belli, Luca; Gaspar, Water B.; Jaswant, Shilpa Singh. (2024) Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54*

Computer Law & Security Review: The International Journal of Technology Law and Practice 54 (2024).

minimum necessary, regulatory interoperability should aim for high levels of protection and compliance.

Interoperability can have different meanings across jurisdictions. As Bacchus et al (2024) observe:

> *For the EU, interoperability means that other jurisdictions must have "adequate" (ie. essentially equivalent) privacy protections enshrined in their legal systems and practices. Meanwhile, some countries in the Asia-Pacific region are prepared to share personal data purely based on voluntary certifications and private undertakings by companies if there is no domestic law.*[89]

Bacchus et al go on to suggest that to be sufficiently interoperable, legal frameworks and governance regimes must take five elements into account: (i) robust legal mechanisms, (ii) rules and safeguards for handling data, (iii) a set of rights for data subjects, (iv) mechanisms for oversight and accountability, and (v) enforcement and redress[90].

Regulatory sandboxes could be useful for testing and developing interoperability mechanisms[91]. Innovative global data governance approaches that draw lessons from other sectors, for example telecommunications and consumer protection, are needed to address current limitations[92].

5.3.1 DATA FREE FLOW WITH TRUST

One initiative related to interoperability is the Data Free Flow with Trust (DFFT) initiative, launched by the presidency of Japan at the 2019 World Economic Forum. DFFT has been described by the OECD as "an international policy drive to promote the use of data for economic and social prosperity, all while effectively managing the associated concerns and challenges"[93]. Though there is no agreed definition of DFFT in the literature, with its focus on challenges for cross-border data flows it may best be understood as combining privacy and security of personal data with enhanced cross-border data flows[94]. In other words, DFFT intends to promote free data flows simultaneously with guaranteeing levels of privacy, to create a more trusted and interoperable global governance system[95].

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

---

[89] Bacchus J, Borchert I, Marita-Jaeger M, Ruiz Diaz J (2024) *Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy* https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy

[90] *ibid.*

[91] Lorrayne Porciuncula, interview conducted for this research, August 9, 2024

[92] *ibid.*

[93] Organisation for Economic Co-operation and Development. (n.d.) *Data free flow with trust*. https://www.oecd.org/digital/data-free-flow-with-trust/

[94] Arasasingham, Aidan; Goodman, Matthew P. (2023) Operationalizing Data Free Flow with Trust (DFFT). *Center for Strategic and International Studies* https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft

[95] Kilic, B (2024) As Global Trade Goes Digital, Trust Becomes Critical. *Centre for International Governance Innovation* https://www.cigionline.org/articles/as-global-trade-goes-digital-trust-becomes-critical/

others[96]. While DFFT is often constructed as a single policy issue, there are multiple issues that need to be addressed to build trust around cross-border transfers[97]. Harmonisation between different jurisdictions through a global treaty on data may be quite difficult to achieve in practice[98].

Although promising[99], a challenge noted[100][101] with the DFFT concept is that it lacks a clear operational framework. In 2023, the G7–under the presidency of the Government of Japan–mandated the OECD's Directorate for Science, Technology and Innovation Committee on Digital Economic Policy to form an Expert Community to inform the creation of a possible operational framework[102]. It is important that the Expert Community includes individuals and organisations from global consumer protection groups so that this crucial perspective is at the heart of ongoing discussions around DFFT.

5.3.2 REGULATORY INTEROPERABILITY AND DATA SOVEREIGNTY

Policy debates on emerging technology often reflect global power dynamics. In order to succeed, regulatory interoperability should not reinforce existing inequalities between upper- and low-/middle-income countries. The inability of states to adhere to common approaches to data protection may particularly affect consumers in low- and middle-income countries, who face even greater difficulty enforcing action against entities from upper-income countries. While economic and social growth have been linked to embracing digital transformation, digitalisation processes can introduce new systemic vulnerabilities that may be exploited by foreign actors[103].

This latter possibility, among other things, has given rise to the idea of data sovereignty, defined as:

> *the capacity [of a nation state] to understand how and why (personal) data are processed and by whom, develop data processing capabilities, and effectively regulate data processing, thus retaining self-determination and control.*[104]

---

[96] Organisation for Economic Co-operation and Development (2023b). *Moving Forward on Data Free Flow With Trust: New evidence and analysis of business experiences*

https://www.oecd-ilibrary.org/docserver/1afab147-en.pdf?expires=1721743428&id=id&accname=guest&checksum=3CF6DF7635057412CAAD229ECA89B380

[97] *ibid.*

[98] World Economic Forum. (2023) *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows* https://www.weforum.org/publications/from-fragmentation-to-coordination-the-case-for-an-institutional-mechanism-for-cross-border-data-flows/

[99] Kati Suominen, interview conducted for this research, August 2, 2024

[100] *ibid.*

[101] Romain Perray, interview conducted for this research, July 30, 2024

[102] G7G20 Documents Database (2023) *Ministerial Declaration - The G7 Digital and Tech Ministers' Meeting* https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting

[103] Belli, Luca; Gaspar, Water B.; Jaswant, Shilpa Singh. (2024) Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54*

[104] *ibid.*

Proponents of data sovereignty claim that it aims to prevent the concentration of value extracted from personal data in upper-income countries, ensuring that nations redefine how the personal data of their citizens may be processed and protected internationally, considered a strategic resource, and used in the national interest[105]. Its detractors worry that pursuing data sovereignty may be a catalyst for data localisation, or even increase the risk of human rights violations[106]. The notion of sovereignty has also been contested. It has been interpreted differently – ranging from national self-determination to absolute state power[107] – according to the actors involved. Some of these interpretations are at odds with the notion of data protection as a fundamental right, as is seen, for example, in the EU[108].

It is argued that regulatory interoperability measures devised collectively with low- and middle-income countries can avoid data localisation, which could thereby minimise the risk of internet fragmentation. According to Belli et al, "being sovereign does not mean being isolated, it means being able to retain full awareness, self-determination and control"[109]. Interpreted this way, data sovereignty is compatible with regulatory interoperability. Enabling data to flow across borders in a secure and trusted manner may even contribute to positive outcomes for digital sovereignty *and* cross-border data flows, by creating regulatory systems that interact with one another while fostering their own unique characteristics–particularly important for consumers in low- and middle-income countries who could have their specific needs addressed[110].

Considering that both the concept of regulatory interoperability and the concept of data sovereignty have elements that can be combined in favour of consumers, it is essential that international initiatives support multilateral and multisectoral collaboration that focuses on the consumer as the central axis of protection[111], safeguarding both the benefits consumers incur from cross-border data flows, and the protection of their personal data. IPDT mechanisms adopted in a given jurisdiction should guarantee sufficient protection for the personal data of consumers, considering the use of this resource in national consumers' best interest, at the same time facilitating international cooperation in order to allow for redress in case of misuse of personal data transferred internationally.

---

[105] *ibid.*

[106] Shahbaz, Adrian; Funk, Allie; Hackl, Andrea. (2020) *User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization.* https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

[107] Braun, Matthias, and Hummel, Patrik (2024) Is digital sovereignty normatively desirable? *Information, Communication and Society 1-14*

[108] Rodotà, S. (2009). Data Protection as a Fundamental Right. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection?. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_3.

[109] Belli, Luca; Gaspar, Water B.; Jaswant, Shilpa Singh. (2024) Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54*

[110] Shahbaz, Adrian; Funk, Allie; Hackl, Andrea. (2020) *User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization.* https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

[111] De La Chapelle, B. and L. Porciuncula (2021). *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*. Internet and Jurisdiction Policy Network https://www.thedatasphere.org//wp-content/uploads/2022/03/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

6. RECOMMENDATIONS FOR INTEROPERABLE AND CONSUMER-CENTRIC REDRESS IN THE EVENT OF MISUSE OF PERSONAL DATA IN IPDT

Despite existing personal data protection frameworks designed to protect personal data internationally, many consumers still face challenges in obtaining meaningful redress. The complexity of international data transfers and the varied implementation of data protection laws contribute to these difficulties, leaving consumers with limited options to exercise their rights properly, address grievances and seek redress.

Based on our analysis of the IPDT mechanisms in relation to the UN's *Guidelines for Consumer Protection*, we offer the following recommendations to strengthen the protection of consumer rights and enhance the overall consumer experience. These recommendations are intended to enable regulatory bodies, policy-makers, international organisations, and industry leaders to take proactive steps to update and refine existing policies related to IPDT structures. We believe that implementing these recommendations will serve to bridge the gap between theoretical protections and practical enforcement, ensuring that consumers have robust mechanisms for addressing violations of their data rights.

RECOMMENDATIONS:

To ensure more effective access to redress for the misuse of their personal data in the context of IPDT, we recommend the following actions are taken:

1. **For all stakeholders: Recognise the growing vulnerability of consumers in the digital age**
   The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor. It is essential that public and private entities consider this in any process for exercising consumer rights, ideally by working with advocates to understand, refine and track definitions, factors and conditions of vulnerability.

2. **For policy-makers and international organisations: Expand international arrangements to harmonise enforcement approaches**
   Policy-makers must ensure that Data Protection Authorities (DPAs) and other relevant authorities can communicate with each other to address complaints. It is important such agreements create a regulatory arrangement with well-defined processes to oversee its enforcement, favouring hard law and clearly defined collaboration mechanisms that promote clarity and certainty across jurisdictions, instead of depending on self-regulation and ad-hoc, unpredictable coordination.

3. **For policy-makers: Strengthen the options for collective redress**
   Strengthening collective redress mechanisms is essential for addressing widespread data protection issues, as collective actions can better enforce rights for many individuals, compared to rare individual legal actions in this field.

4. **For policy-makers and the private sector: Invest in and experiment with additional informal pathways to conflict resolution**
   Examples include online dispute resolution platforms and data fiduciaries. The existence of informal redress mechanisms should not preclude or replace a consumer's right to access to justice via formal means.

5. **For policy-makers and international organisations: Treat consumers equitably across jurisdictions**
   Develop regulations that support equitable treatment for consumers with different citizenship status, regardless of their nationality or the jurisdiction that is enforcing their rights, when they seek redress for violations arising from international data transfers. Stakeholders should aim to reflect the highest consumer and data protection standards available, rather than the lowest common denominator.

6. **For international organisations: Continue to pursue regulatory interoperability in the context of a free and open internet**
   Direct efforts towards establishing multilateral and bilateral agreements to facilitate rights-respecting IPDTs, putting consumers' access to redress at the centre of discussions:

   a. Employ a multistakeholder approach (see recommendation 7.) to ensure that interoperability alternatives consider multiple contexts and vulnerabilities;

   b. Respect digital sovereignty and ensure regulations resulting from such agreements consider multiple jurisdictions, and are not simply imposed on low- and middle-income countries by upper-income countries;

   c. Establish transborder regulatory sandboxes in spaces of power such as the OECD and UN, to allow different stakeholders to test and improve the benefits and limits of old and new frameworks of personal data protection;

   d. Where appropriate, provide financial incentives to enable low-income countries to operationalise such agreements.

7. **For international organisations: Consult with civil society and consumer protection bodies**
   In directing efforts towards regulatory interoperability, include a public process of gathering inputs on the local reality of each country, facilitating the creation of regulations that are effective locally and, consequently, globally.

8. **For the private sector: Invest in transparency and the provision of appropriate information to empower consumers in making informed decisions** Enhance consumer awareness about available mechanisms for redress, by providing transparent information that is relevant, timely and inclusive. Such efforts should not preclude appropriate and ongoing investment in data privacy and security to protect consumers.

9. **For regulatory bodies and the private sector: Use technology to facilitate the exercise of rights**
   Invest in technologies that facilitate the exercise of rights, especially in countries where digital literacy is lower. Ensure these technologies have undergone testing and impact assessments prior to being made available for consumer use, and on an ongoing basis. These arrangements should not preclude access to human assistance.

10. **For policy-makers and the private sector: Explore the possibility of a collective fund for redress contributed to by private companies**
    Incentivise private companies to create a fund for redress for consumers. Such a fund, overseen by a multistakeholder board to decide the different cases, should be tasked to ensure that its outcomes are consumer-centred.

7. CONCLUSION

This report has unearthed a significant gap between the theoretical protections offered by international data protection frameworks, and the practical realities faced by consumers seeking redress internationally. The complexities of international data transfers and the inconsistent implementation of data protection laws contribute to the challenges consumers encounter in exercising their rights effectively.

By adopting the recommendations contained within this report, policy-makers, regulatory bodies, and industry leaders can strengthen the protection of consumer rights and ensure that redress alternatives are both effective and accessible. This holistic approach will contribute to a more equitable and responsive data protection landscape, ultimately enhancing consumer trust and confidence in international data practices.

The protection of consumers' personal data rights is a critical concern in the context of IPDT. The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor. Because IPDTs have become integral to trade expansion and economic growth, it is imperative that the utmost care is taken to protect consumers, so as not to undermine confidence in the global economy.

8. ACKNOWLEDGEMENTS

This report was a collaborative effort led by Consumers International and its Digital Consumer Rights programme team. We are grateful to the Ford Foundation for funding the programme. The research underpinning this report was prepared by Payne & Routledge and contributed to by a global, multistakeholder group of experts and practitioners representing Consumers International Members, academia, civil society and businesses. We are thankful to them for offering their time and expertise in support of this work.

Authors

Maraísa Cezarino, Researcher, Payne & Routledge
Hannah Draper, Director, Payne & Routledge
Marina Garrote, Researcher, Payne & Routledge
Paula Guedes, Digital Rights Policy Advisor and Researcher, Payne & Routledge
Javier Ruiz Diaz, Senior Digital Rights Advisor, Consumers International

Contributors

Kimberly Bella, Senior Director, Global Data Office, Visa
Kendall Brent, Strategic Analyst, Market Development and Data Commercialization, Visa
Joao Pedro Cezarino, Independent Technical Advisor
Aayushi Chaturvedi, Consumer Insights Lead, Consumers International
Fiorentina García Miramón, Co-Founder, Tec-Check
Paulina Gutiérrez, Independent Policy and Strategy Consultant
Stefan Hall, Director, Digital Innovation and Impact, Consumers International
Becky Hogge, Editor
Burcu Kilic, Senior Fellow, Centre for International Governance Innovation
Juliana Mozachi Sandri, Head, Department of Conduct Supervision, Central Bank of Brazil
Michael Nunes, Vice President, Global Policy, Visa
Romain Perray, Partner, McDermott Will & Emery
Lorrayne Porciuncula, Co-founder and Executive Director, Datasphere Initiative
Maximilian Schrems, Founder and Chair, European Center for Digital Rights (NOYB)
Gabrielle Shea, Global Public Policy Manager, Visa
Kati Suominen, Founder and Chief Executive Officer, Nextrade Group
Lux Teixeira, Chief Executive Officer and Principal, Mycelium Tecnologia
Michael Terry, Editor

9. REFERENCES

Arasasingham, Aidan; Goodman, Matthew P. (2023) Operationalizing Data Free Flow with Trust (DFFT). *Center for Strategic and International Studies.* https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft.

Article 29 Data Protection Working Party (2017). *Guidelines on consent under Regulation 2016/679* https://ec.europa.eu/newsroom/article29/redirection/document/51030.

Asia-Pacific Economic Cooperation (2005) *APEC Privacy Framework.* https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf.

Asia-Pacific Economic Cooperation (n.d.) APEC Cooperation Arrangement For Cross-Border Privacy Enforcement. https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf.

Bacchus J, Borchert I, Marita-Jaeger M, Ruiz Diaz J (2024) *Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy.* https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy.

Belli, Luca; Gaspar, Water B.; Jaswant, Shilpa Singh. (2024) Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54.*

BBC News (2020) *EU-US Privacy Shield for data struck down by court*. https://www.bbc.co.uk/news/technology-53418898.

Braun, Matthias, and Hummel, Patrik (2024) Is digital sovereignty normatively desirable? *Information, Communication and Society 1-14*

Brazilian General Data Protection Law (LGPD). https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

Cadwalladr, C (2017) The great British Brexit robbery: how our democracy was hijacked. *The Guardian.* https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Carroll, D (2022) David Carroll: Cambridge Analytica & Data Privacy (Steven Parton, interviewer). Singularity podcast https://www.su.org/resources/cambridge-analytica-data-privacy.

Center for Global Development (2021) *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity.* https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and.

Centre for Information Policy Leadership (2022) *Local Law Assessments and Online Services – Refining the Approach to Beneficial and Privacy-Protective Cross-Border Data Flows.* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_-_local_law_assessments_and_online_services_-_a_case_study_from_british_columbia__10_june_2022_.pdf.

Consumers International (n.d.) *What We Do: Our Consumer Protection and Empowerment Index: a Unique Tool to Guide Marketplace Change.* https://www.consumersinternational.org/what-we-do/the-global-index/.

Consumers International (2024) *Transparent Digital Finance for Consumers.* https://www.consumersinternational.org/media/534803/transparent-digital-finance-for-consumers.pdf

Council of Europe. (2018) *Convention 108 + Convention for the protection of individuals with regard to the processing of personal data.* https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Court of Justice of the European Union (2020) *Case C-311/18 (Schrems II).* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en.

Custers, Bart; Schermer, Bart Willem; Van Der Hof, Simone (2014). *The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection*. Leiden University Faculty of Law, Ethics & Information Technology.

Data Guidance (n.d.) https://www.dataguidance.com/.

Data Privacy Framework Program (n.d.) *Data Privacy Framework List.* https://www.dataprivacyframework.gov/list.

Data Privacy Framework Program (n.d.) *How to Submit a Complaint Relating to a Participating Organization's Compliance with the DPF Principles.* https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization%E2%80%99s-Compliance-with-the-DPF-Principles.

Data Privacy Framework Program (n.d.) *6–Self Certification.* https://www.dataprivacyframework.gov/framework-article/6%E2%80%93Self-Certification,

Davies, H (2015) Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian.* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

De La Chapelle, B. and L. Porciuncula (2021). *We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty*. Internet and Jurisdiction Policy Network. https://www.thedatasphere.org//wp-content/uploads/2022/03/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf.

Dolan, Jonathan; Satapathy, Sarthak; Sabiti, Bernard (2024). Data can drive shared prosperity for governments, businesses, and citizens: unlocking it requires trusted data exchange. *Digital Impact Alliance.* https://dial.global/research/data-can-drive-shared-prosperity-it-requires-trusted-data-exchange/.

European Agency for Fundamental Rights (2014). *Access to data protection remedies in EU Member States*. https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states.

European Commission (n.d.) *New Standard Contractual Clauses - Questions and Answers overview.* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions.

European Commission (2021). *Standard Contractual Clauses (SCC)*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

European Data Protection Board (2018) *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

European Data Protection Board (2020a). *Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1.* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Board (2020b). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://www.edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Data Protection Board (2023) *1.2 billion euro fine for Facebook as a result of EDPB binding decision.* https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

Frajhof, Isabella Z.; Sombra, Thiago Luís. (2020) A transferência internacional de dados pessoais. In: Mulholland, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélogo, pp. 265-288.

G7G20 Documents Database (2023) *Ministerial Declaration - The G7 Digital and Tech Ministers' Meeting.* https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting.

Garcia Arabehety, Pablo, Gregory Chen, William Cook, and Claudia McKay (2016) Digital Finance Interoperability & Financial Inclusion: A 20-Country Scan. Working Paper. Washington, D.C.: CGAP.Tr.

General Data Protection Regulation (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679.

Gov.br (2018) Lei Nº 13.709, August 14 2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Gov.br (2024) Resolução Cd/ANPD Nº 19, De 23 De Agosto De 2024. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396.

Information Commissioner's Office (n.d.). *Transfer risk assessments.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/.

International Centre for Dispute Resolution American Arbitration Association (n.d.) The EU-U.S. DPF and UK Extension to the EU-U.S. DPF Annex I Binding Arbitration Mechanism. https://go.adr.org/dpfeufiling.html.

International Monetary Fund (2021) *Toward a Global Approach to Data in the Digital Age.* https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264.

Kilic, B (2024) As Global Trade Goes Digital, Trust Becomes Critical. *Centre for International Governance Innovation.* https://www.cigionline.org/articles/as-global-trade-goes-digital-trust-becomes-critical/.

Marelli, Massimo. (2024) Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms. *International Data Privacy Law,* Vol. 14, No. 1.

MIT (n.d.) MIT Future of Data Initiative. https://futureofdata.mit.edu/.

Organisation for Economic Co-operation and Development. (n.d.) *Data free flow with trust*. https://www.oecd.org/digital/data-free-flow-with-trust/.

Organisation for Economic Co-operation and Development (n.d.). *Cross-border data flows.* https://www.oecd.org/en/topics/cross-border-data-flows.html.

Organisation for Economic Co-operation and Development (2001). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf.

Organisation for Economic Co-operation and Development (2020). Data localisation trends and challenges. *OECD Digital Economy Papers No. 301,* OECD Publishing, Paris

Organisation for Economic Co-operation and Development. (2023a). Consumer vulnerability in the digital age. *OECD Digital Economy Papers, No. 355*, OECD Publishing, Paris.

Organisation for Economic Co-operation and Development (2023b). *Moving Forward on Data Free Flow With Trust: New evidence and analysis of business experiences.* https://www.oecd-ilibrary.org/docserver/1afab147-en.pdf?expires=1721743428&id=id&accname=guest&checksum=3CF6DF7635057412CAAD229ECA89B380.

Red-Iberoamericana de Proteccion de Datos (2017) Standards For Personal Data Protection For Ibero-American States. https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf.

Red-Iberoamericana de Proteccion de Datos (2021). *Recommendations for the processing of personal data through cloud computing services*. https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf.

Red-Iberoamericana de Proteccion de Datos (2023a) *Annex: Model Contractual Clauses.* https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf.

Red-Iberoamericana de Proteccion de Datos (2023b) *Implementation Guide: On Model Contractual Clauses for International Personal Data Transfers (IPDT).* https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-en.pdf.

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

Reifa, C and Coll, L (2024) *The transformative potential of Enforcement Technology (EnfTech) in consumer law* *https://static1.squarespace.com/static/638646cea1515c69b8f572cb/t/65a522dbeafaaf1208982746/1705321180457/EnfTech_final+report_2024.pdf*

Robinson, Lisa; Kizawa, Kosuke; Ronchi, Elettra. *Interoperability of privacy and data protection frameworks. Going Digital Toolkit Note.* http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf.

Rodotà, S. (2009). Data Protection as a Fundamental Right. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection?. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_3.

Shahbaz, Adrian; Funk, Allie; Hackl, Andrea. (2020) *User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization.* https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.

Solove, Daniel J.; Citron Danielle Keats (2021) *Privacy Harms.* https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications.

Sullivan, C (2019) EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era, *Computer Law & Security Review*, 35 (4), pp 380-397.

UNESCO (2018) *Guidelines for Designing Inclusive Digital Solutions and Developing Digital Skills.* https://www.unesco.org/en/articles/unesco-launches-guidelines-inclusive-digital-solutions-people-low-skills-and-low-literacy.

United Nations (2016) Guidelines For Consumer Protection. https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf.

United Nations Conference on Trade and Development (2016) *Data protection regulations and international data flows: Implications for trade and development.* https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf.

US Federal Trade Commission. (2019) *Opinion of the Commission, Docket no. 9383.* https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf.

US Department of Commerce (n.d.) *Global Cross-Border Privacy Rules Declaration.* https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

US Supreme Court (2021) *TransUnion LLC v. Ramirez, 594 U.S. (2021).* https://supreme.justia.com/cases/federal/us/594/20-297/.

van Geuns, J and Brandusescu, A (2020) Shifting Power Through Data Governance Mozilla Insights. https://assets.mofoprod.net/network/documents/ShiftingPower.pdf.

Visa (n.d.). *Consent Management Guidelines.* https://globalclient.visa.com/ConsentManagement.

Visa Consumer Empowerment Research (n.d.) *The Role of Consumer Consent and Regulatory Interoperability in Building a Trusted Digital Economy.* https://images.globalclient.visa.com/Web/InovantElqVisaCheckout/%7B6e2ee1cf-1605-4044-a6ce-cee57e5053a3%7D_Visa_The_Role_of_Consumer_Consent_and_Regulatory_Interoperability.pdf.

Visa (2024) *Consumer Empowerment Study*. https://globalclient.visa.com/ConsentManagement.

Wakefield, J (2018) Cambridge Analytica taken to court over data storage *BBC News.* https://www.bbc.com/news/technology-43501184.

World Economic Forum. (2023) *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows.* https://www.weforum.org/publications/from-fragmentation-to-coordination-the-case-for-an-institutional-mechanism-for-cross-border-data-flows/.

10. ANNEXES

ANNEXE I – IPDT MECHANISMS WITHIN THE REVIEWED JURISDICTIONS

The chart below provides an overview of the jurisdictions where the lawful mechanisms for IPDT selected for review in this study are applicable. (Please note *consent* is broadly used as a lawful mechanism for IPDT beyond the jurisdictions reviewed here.)

Lawful mechanism for IPDT	Consent	LGPD's SCCs	GDPR's SCCs	Red Iberoamericana's SCCs	EU-US Data Privacy Framework	APEC Cross Border Privacy Rules
Australia	x					x
Brazil	x	x		x		
Canada	x			x		x
Chinese Taipei	x					x
Spain	x		x	x	x	
Portugal	x		x	x	x	
Other EU countries	x		x		x	
Japan	x					x
Mexico	x			x		x
Singapore	x					x
USA	x				x	x
Kenya	x					
South Africa	x					
South Korea	x					x
Philippines	x					x

@Consumers International