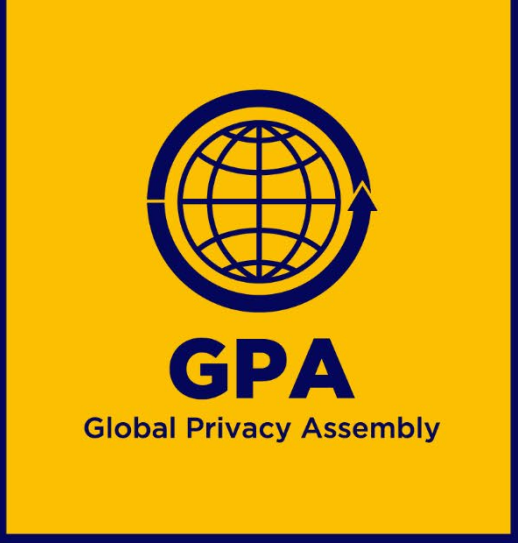

Global Frameworks and Standards Working Group

Report – July 2022

Chair authority: UK Information Commissioner's Office

Table of Contents

Executive Summary

The Global Frameworks and Standards Working Group (GFSWG, formerly the Policy Strategy Working Group Workstream 1) has made good progress in 2021-22 in contributing towards the delivery of the GPA's strategic priorities and plan.

Building on our comprehensive analysis of global privacy and data protection frameworks from 2020, and our supplementary pieces of work on cross border transfers and data protection terms and their meanings in 2021, we have continued to develop our work on cross border transfers, have now completed our work on data protection terms and have started a new piece of work to articulate the GPA's view of high data protection and privacy standards.

High standards of data protection and privacy

In 2021-22, the GFSWG has started work on an allocated action from the GPA's Strategic Plan 2021-23[1] to work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards. This goes to the core of the GPA's work, as the setting out of a common view on high standards will support regulatory cooperation, as well as promote high standards globally. The GFSWG has carried out foundational work on this item in 2021-22, and we aim to submit a resolution or policy statement on high standards in 2023.

Cross border transfers and mechanisms

In line with GPA priorities, the GFSWG recognises the importance of protecting personal data wherever it flows as the global digital economy continues to develop, and we continue to work on this topic to support the secure and smooth flow of personal data across borders. In 2021-22, the GFSWG has continued to build on work relating to cross border transfers, to assist authorities and stakeholders better understand available mechanisms and current issues. We have completed a literature review and report, are currently working on more detailed analyses and comparisons of transfer mechanisms, and will continue this into 2023. We are also considering developing a repository of helpful documents in 2023.

Data protection terms and their meanings

The GFSWG has worked over the past two years to analyse and understand what is meant by core data protection and privacy terms, and to develop shared meanings. In 2021-22 we have added to our existing list of core terms with a list of data protection principles and their meanings, and have

[1] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

collated the shared meanings of both core terms and principles into a glossary to publish on the GPA website. This work is now completed.

Stakeholder engagement

The GFSWG has engaged with other GPA member authorities, the GPA Reference Panel and other organisations such as the OECD in our work this year. We will continue to map and identify other stakeholders to engage with to enhance our work, and to promote it, as needed in 2023.

At this half way point in the current GPA Strategic Plan 2021-23, the GFSWG submits this annual report, and other outputs from the above work items in annexes, for adoption by the Closed Session.

Introduction

Global frameworks and standards is key to the GPA's delivery of its first strategic priority – to advance global privacy in an age of accelerated digitalisation, as the GPA continues to work towards a global regulatory environment with clear and consistently high standards of data protection. The importance of global frameworks and standards in promoting high standards of data protection and privacy also supports convergence and interoperability, and the flow of data across borders.

The Global Frameworks and Standards Working Group (GFSWG, formerly the Policy Strategy Working Group, Workstream 1) is close to completing its third year of operation. Its original mandate was to deliver actions from the GPA 2019-21 Policy Strategy (which can be found in the annex to the Resolution on the Conference's Strategic Direction 2019-21[2], adopted in Tirana in October 2019) – most notably the completion of an analysis of global privacy and data protection frameworks.

That analysis was adopted in 2020, and in 2021 the GFSWG was given a further mandate in the adopted Resolution on the Assembly's Strategic Direction 2021-23[3], to deliver actions set out to implement the GPA's Strategic Plan for 2021-23, in addition to continuing to build on earlier work.

GFSWG has worked on the following items in 2021-22:

- **Work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards.**

A common view of what is meant by high data protection and privacy standards can support regulatory cooperation, so is at the core of much of the GPA's work. This action is therefore a significant one, and it will be important to take an inclusive approach to ensure that wider member views are taken into account. For this reason, in 2021-22 GFSWG started foundational work towards this action, and we plan to continue the work and submit a resolution or policy statement for adoption in 2023.

- **Continue work on cross border transfer mechanisms**

The need to protect personal data wherever it flows is especially important as the global digital economy continues to develop, and the GPA continues to be keen to do what it can to support the secure and smooth flow of personal data across borders. After delivering a high-level analysis and report on transfer mechanisms in 2021, GFSWG has continued to build on that work by undertaking a literature review and associated report, in order to understand where the GPA can add value in this area in its future work. The document also serves as a helpful reference document for others

[2] Resolution on the Conference Strategic Direction 2019 - 2021 FINAL (globalprivacyassembly.org)
[3] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

interested in the development of global approaches to cross border transfers. Work has also begun to analyse and explain transfer mechanisms in more detail, with a comparison of the contractual clause mechanisms in the EU GDPR, the UK's IDTA, the ASEAN and RIPD clauses.

- **Continue the rolling programme to develop common definitions of what is meant by key data protection terms.**

Much of the GFSWG's work to date has focused on identifying commonality in global and regional privacy and data protection frameworks. A related activity has been to understand what is meant by key terms in those frameworks and instruments, and to identify where shared meanings exist. After adopting a set of common meanings of core data protection terms in 2020, in 2021-22 the GFSWG focused on the meaning of terms relating to core data protection principles. This involved analysis of the descriptions of principles in global data protection frameworks and instruments, the identification of commonalities and the development of common meanings.

- **Develop formalised relationships with other fora undertaking similar work, taking into account work done by SDSC on stakeholder engagement where appropriate.**

The GFSWG has engaged with several stakeholders in 2021-22, such as OECD, to consider where our work aligns. We have also made enquiries of the GPA Reference Panel of experts. Further stakeholder engagement will take place in 2022-23.

More detail, including further reports and outputs in relation to the above work items can be found in the next section and in annexes to this report.

The GFSWG Chair's representative attended a 'deep dive' meeting with the GPA ExCo's Strategic Direction Sub-Committee (SDSC) in March 2022. During this meeting a presentation was made to SDSC on progress made, questions answered and feedback received. In particular, it was noted that there was some intersection between the GFSWG work on high data protection standards and the work of the Data Protection and other Rights and Freedoms WG, which explored opportunities for convergence around existing data protection instruments in its 2021 adopted narrative on privacy and data protection as fundamental rights. The GFSWG will engage with other GPA working groups as needed to ensure that opportunities for alignment are considered as our work progresses.

Working Group members

UK ICO (Chair)	OAIC Australia	OPC Canada	Côte d'Ivoire
Council of Europe DPC	Dubai IFC	EDPS	CNIL France
Gabon	Germany BfDI	Israel	PPC Japan
Korea PIPC	INAI Mexico	OPC New Zealand	Ontario IPC
NPC Philippines	Portugal	San Marino	Senegal
Spain	Switzerland FDPIC	KVKK Turkey	US FTC
Uruguay	European Commission (observer)	European Data Protection Board (observer)	OECD (observer)

Working Group Activities

The GFSWG's activities in 2021-22 have centred around the work items listed above in the introduction section. In more detail, those activities have included:

- **Work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards.**

As mentioned in the previous section, a common view of what is meant by high data protection and privacy standards could provide substantial underlying support for the GPA's achievement of its vision and mission. This action is important to get right, balancing an appropriate level of ambition while producing an output the GPA's wider membership will be able to support.

In 2021-22 the GFSWG has carried out activities to form the foundation of our eventual output. As a first step, we considered similar work carried out previously by the GPA. The Madrid Resolution[4], adopted in 2009, is the most recent example of GPA document which sets out the Assembly's views on high general data protection and privacy standards, as opposed to in relation to particular activities. A review of the Madrid Resolution was carried out – to consider the standards set out in that document, and to consider what was missing – that is, what principles, rights and other elements might the GPA wish to advocate for now in addition to those adopted in the Madrid Resolution in 2009?

While this work is still ongoing, initial findings indicate that the Madrid Resolution's content is quite comprehensive and forward-thinking, including some important provisions that would still be agreed today as exemplifying high standards. Key principles are covered, accountability measures receive appropriate attention, and the importance of an independent and impartial supervisory authority is emphasised. There is also a clear expectation that principles and rights should only be restricted by states when necessary and only in certain circumstances, as provided for by national legislation which establishes appropriate guarantees and limits to preserve individuals' rights.

We then compared the provisions of the Madrid Resolution with other current global frameworks and more newly-developed instruments, and identified some elements that were missing or not substantively covered by the former. We also considered whether those 'missing' elements had featured substantively in the work of international or multilateral organisations, to assist in indicating their importance and current relevance.

We have recently engaged with a few GPA members and other stakeholders to obtain their views, and at the time of writing are developing a survey for all GPA members to complete. The aim is that the review, together with member feedback, will identify elements of practical importance to authorities now and in the future, to inform the drafting of the resolution or policy statement in 2023.

[4] 14302 STANDARS.qxp:Maquetación 1 (globalprivacyassembly.org)

- **Continue work on cross border transfer mechanisms**

In 2021 GFSWG adopted with its annual report a high-level analysis and report on commonalities between transfer mechanisms. The report suggested that the GPA 'may wish to consider what other pieces of comparative analysis have been done by other bodies on transfer mechanisms, and whether there are any gaps in this respect that could benefit from further work by the GPA'.

Consequently, in 2022, the GFSWG carried out a literature review of similar work undertaken by other key stakeholders in order to identify any gaps or opportunities for further work by the GPA.

The literature review considered documents from all global regions, and included several reports and papers from international/multilateral organisations, such as the OECD, UNCTAD and WEF, as well as articles and selected pieces of guidance. Key points from the documents were summarised, and a report was produced, which identified several high-level themes, and possible areas of interest for the GFSWG's work in 2022-2023.

In summary, the headline themes noted the existence of:

- convergence in global frameworks, largely acknowledged as a positive in enabling cross border transfers;
- a potential role for global standards and/or international frameworks;
- an emphasis on tools and mechanisms, including:
    - A proliferation of new and existing mechanisms, with some developing concern about complexity and the cost of compliance;
    - Contractual clauses being the most prominent mechanism, but an increased interest was noted in codes and certification as transfer mechanisms;
- new developments including Global Cross Border Privacy Rules;
- the potential role of technology-driven initiatives to enable greater trust in cross border data flows;
- developing approaches in China and India as new data protection and privacy regimes emerge; and
- areas of concern, such as data localisation and government access to data and implications for trusted data flows.

Findings indicated that there were opportunities for further GPA work on this topic, which could aim to:

- aid further understanding of current and emerging transfer mechanisms;
- highlight commonality and convergence;
- monitor developments; and

- foster engagement with global networks, multilateral organisations and other key stakeholders in order to support the above opportunities.

Some of this work has already begun in the form of a comparison of contractual clauses in the EU, UK, ASEAN countries and the RIPD (Ibero-American Network) in order to understand the commonalities and differences between the clauses in different global regions.

The literature review and report can be found at Annexes A and B.

- **Continue the rolling programme to develop common definitions of what is meant by key data protection terms.**

The aim of this work item has been to understand what is meant by key terms in global data protection frameworks and instruments, and to identify and highlight where shared meanings exist. After adopting a set of common meanings of core data protection terms in 2020, in 2021-22 the GFSWG focused on the meaning of terms relating to core data protection principles. This involved further analysis of global data protection frameworks and instruments, and the development of common meanings. Commonalities were identified and shared meanings drafted for the following principles: fairness; lawfulness; purpose specification; proportionality; data quality; transparency; accountability; security; and data retention.

Finally, a glossary document has been developed which includes the agreed meanings of the core data protection terms adopted in 2021, and the meanings of the principles listed above, and once adopted we will engage with the GPA Secretariat to arrange an appropriate location for publication on the GPA website.

The analysis, report and glossary document can be found at Annexes C and D.

- **Develop formalised relationships with other fora undertaking similar work, taking into account work done by SDSC on stakeholder engagement where appropriate.**

The GFSWG has engaged with several stakeholders in 2021-22, such as OECD, to consider where our work aligns. We have also made enquiries of the GPA Reference Panel of experts. Further stakeholder engagement will take place in 2022-23, and will take into account any relevant output from the SDSC as and when available.

Forward looking plan 2022-2023

The current GPA Strategic Plan 2021-23[5] notes the need for mechanisms to ensure that personal data is protected wherever it is processed and flows, the importance of promoting high standards of data protection and privacy, and the role the GPA can play in doing this.

As per the Plan, in 2022-23 the GFSWG will continue work on the following items:

- **Work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards.**

This will involve finalising and circulating the GPA member survey for their views of high data protection and privacy standards. Work will then focus on developing and engaging with members on the draft resolution or policy statement to be submitted in 2023.

- **Continue work on cross border transfer mechanisms**

This will involve aiding understanding of current and emerging mechanisms, by carrying our further comparative work on various types of mechanism. GFSWG will also consider collating a repository of helpful documents to assist understanding of transfer mechanisms and related issues. Finally, we will continue to monitor developments of new mechanisms and frameworks.

- **Develop formalised relationships with other fora undertaking similar work, taking into account work done by SDSC on stakeholder engagement where appropriate.**

In the context of our work items above, we will renew efforts to map and engage with stakeholders outside the GPA, especially those undertaking similar work.

[5] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

Conclusion

In 2021-22, the GFSWG has made good progress against our work plan and actions allocated to us by the GPA Strategic Plan 2021-23. We have:

- Started foundational work in preparation for submitting a GPA resolution or policy statement to articulate the GPA's view of high data protection and privacy standards;
- Carried out further work on cross border transfers and mechanisms, and have completed a literature review and report.
- Delivered the second and final phase of work on data protection terms, delivering a list of shared meanings of terms relating to data protection principles, and a glossary to put the first and second-phase lists of terms and their meanings together for publication on the GPS website.

As global frameworks and standards continues to be a crucial element of the GPA's work towards a global regulatory environment with clear and consistently high standards of data protection, we look forward to continuing to progress in 2022-23.

The chair would like thank the members of the Working Group, and in particular those who have worked within the sub groups, for their contributions this year.

Annexes

Annex A: Literature review on cross border transfers - report

GPA GLOBAL FRAMEWORKS AND STANDARDS WORKING GROUP (GFSWG)

Literature review on cross border transfers

1. Introduction

Cross border transfers, and the tools and mechanisms used to facilitate such transfers in order to comply with data protection and privacy requirements, are a continued area of interest to authorities and many of their stakeholders.

In the Global Frameworks and Standards Working Group's (GFSWG, formerly the Policy Strategy WG1) 2020 analysis of global data protection and privacy frameworks, it was unsurprising to find broad agreement across most frameworks in relation to a general principle of the need to protect personal data across borders.

In 2021 this was followed by a further analysis and report on cross border transfer mechanisms. This work found a variety of mechanisms provided for by global data protection and privacy frameworks, considered them at a high level and highlighted commonalities with some mechanisms being found in several of the frameworks. The concept of equivalence, use of contractual clauses and binding corporate rules were common to several frameworks, although there were differences in implementation, with some frameworks not including any details on how this should be done. The report noted that some mechanisms, such as certification and codes, were quite new and that further commonality might emerge as they developed.

In 2022, to build on the above work, the GFSWG has worked on a literature review on the topic of cross border transfers. The 2021 report noted that it would be helpful to consider any other pieces of comparative analysis done on transfer mechanisms, and during initial desk based research to identify other work, the WG noted that there were a large number of papers, reports, articles and guidance pieces already published on transfer mechanisms but also on general issues relating to cross border transfers. The literature review was, for this reason, quite broad, ultimately considering several reports and papers from international / multilateral organisations such as the OECD, UNCTAD and WEF, as well as articles and selected pieces of guidance.

2. Literature review summary, and key themes and issues identified

A total of 38 documents, produced by 27 organisations and assessing all global regions , were reviewed. Detail of the documents reviewed, with individual document summaries and links, are

listed in Annex A. While it can be a challenge to summarise such a broad range of documents, the review identified several high-level themes occurring in the documents reviewed, as follows:

- **Convergence** was noted in global frameworks

Several of the documents reviewed identified or appeared to support the existence of similarities across frameworks in terms of regulatory approaches and the mechanisms available, and several noted at least some level of convergence across jurisdictions on particular transfer mechanism approaches. However the lack of a global level policy discussion on interoperability was noted in some reports.

- Potential role for **global standards / international frameworks**

The UNCTAD digital economy report included a suggestion that there is a **need for global governance of cross border data flows**, complementing measures taken at other levels of governance. The report argued that there was a patchwork of national regulations, with no satisfactory solution at regional or international level. It suggested the need for international collaboration to develop a global policy approach.

Others (eg OECD) concluded it was the prerogative of national governments to establish the mix of instruments or mechanisms that best serve their policy objectives, but noted that greater understanding, discussion and agreement on these instruments could be conducive to greater overall confidence and trust. On a different level, away from the focus on regulatory instruments by governments, the OECD report also noted standards developed by non-governmental and private sector organisations used as tools to address privacy and data protection issues relating to cross border data flows. International Organization for Standardization (ISO) privacy and data protection standards were highlighted as examples of this.

- **An emphasis on tools and mechanisms**

Many of the documents discussed aspects of cross border tools and mechanisms, such as:

  - The **proliferation of existing and new mechanisms**. New tools and mechanisms were being developed with, for example, new and amended standard contractual clauses being identified across several frameworks. While the broader availability of new protections provides obvious benefits, there were some issues raised:
    - **Complexity and the cost of compliance**. Organisations working across several jurisdictions need to understand the different mechanisms and comply accordingly. The degree of convergence mentioned above means that some similarity between mechanisms exists, which is helpful, but some documents

noted that differences between jurisdictional approaches and mechanisms leads to increased costs.

- Some documents therefore focus on understanding the detail of the various mechanisms, and indicate that a more detailed analysis of different kinds of transfer mechanisms across the frameworks would be helpful in developing understanding and highlighting commonalities, and could assist authorities as they are tasked with implementing new mechanisms in their jurisdictions, as well as helping organisations in their goal of compliance.

- With the **increasing number of tools and mechanisms being developed** comes the potential for new mechanisms or even new frameworks. In addition to the issues above, this emphasises the importance of interoperability. A development of particular interest is the establishment of the Global Cross-Border Privacy Rules Forum. The Forum's stated objective is establishing an international certification system based on the APEC Cross Border Privacy Rules, while promoting interoperability with other frameworks. This is an emerging development noted in the documents that should be monitored.

- Equivalence and standard contractual clauses appeared to be the most prominent mechanisms discussed.

- **Increased interest in codes and certification as transfer mechanisms.** As mechanisms common to several frameworks, these are highlighted in some documents as potential areas for convergence, but as still relatively new mechanisms yet to be fully implemented. Developments relating to these mechanisms should be monitored.

- **Potential role of technology**

The OECD report notes that technology-driven initiatives such as privacy enhancing technologies (PETs, such as cryptography technologies and data sandboxes, which enable access to data within controlled environments) are increasingly being used by organisations to protect and control access to data, and may enable greater trust in cross border data flows.

- **A keen interest in the developing approaches in China and India and their potential impact**

Several documents focused on developments of new laws in China and India, noting the potential impact on global data flows, some areas of commonality with existing approaches and some

concerns around certain elements such as data localisation requirements. As implementation approaches develop, this should be monitored.

- **Concerns with increased interest in and use of data localisation**

As indicated above, some documents note a level of concern in the increased interest in data localisation in some frameworks and jurisdictions.

- **Concerns with government access to data and implications for trusted data flows**

Several documents refer to the OECD's work on government access to data, and to the GPA resolution on the same topic.

Conclusion and next steps

While there is a large body of work relating to cross border transfers already published, the literature review carried out indicates that there are areas that the GPA could helpfully focus on. The GPA should work to aid further understanding of current and emerging mechanisms, highlighting commonality and convergence, and engaging with networks, multilateral organisations and other stakeholders as they develop approaches. This could be done by more detailed comparative analysis of mechanisms where such work does not already exist, and the monitoring of emerging and future mechanisms, by horizon scanning of reports, articles and announcements, together with engagement with key stakeholders, such as the Council of Europe, Global CBPR Forum and other relevant bodies.

Annex B: Literature review on cross border transfers – table of reviewed documents

GPA Global Frameworks and Standards Working Group (GFSWG) Work Item 2:

Continued work on cross border transfers

Literature Review 2022

GPA GFSWG Literature Review: Reports on Cross-Border Data Flows and Transfer Mechanisms

No.	Organisation	Title	Content summary, main points made and/or issues raised (relating to cross-border transfers of personal data)	Conclusions/Recommendations	Link
General reports / papers					
1.	**Global Privacy Assembly (GPA)**	**Policy Strategy Working Group 1: Global Frameworks and Standards Annual Report. (Annex A: Report on cross border transfer mechanisms)** **Published October 2021.**	The report analysed cross border transfer mechanisms from ten global data protection frameworks: • All frameworks shared common principles relating to cross-border transfers, in particular the principle that transfers can take place if appropriate levels of protection are in place. • Additionally surveyed GPA members on transfer mechanisms contained in	• The analysis found several areas of convergence in the global frameworks and national laws considered - particularly in the concepts of equivalence, contractual clauses and BCRs. • Newer GDPR mechanisms such as codes and certification schemes might become more prevalent in time, and	1.3b-version-4.0-Policy Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org) (Annex A, pages 14-27)

			their domestic data protection regimes.
			
			• Identified the following mechanisms in the frameworks:
			  ○ Equivalence / adequacy – present in 8/10 frameworks, though to differing degrees of detail, with most frameworks not specifying how such mechanisms should work.
			  ○ Contractual safeguards between transferring and recipient organisations – a major area of commonality.
			  ○ Self-assessment schemes – only present in three frameworks with the APEC CBPR system being the best known; not an area of any significant commonality. Future approved certification systems under the GDPR may be included here.
				might increase commonality with the APEC CBPR system.
				
				• Overall, the analysis found a relatively consistent set of mechanisms that jurisdictions developing/implementing a transfers framework could find useful to consider aligning with.
				
				• Next steps could involve:
				  ○ Monitor the development of codes and certification as transfer mechanisms.
				  ○ Further consideration of potential commonalities between the GDPR's approved certification scheme mechanism and the APEC CBPR system.	

			○ Binding corporate rules (BCRs) – specifically mentioned in two frameworks, more generally in one, with a further three referring to measures in general that could include BCRs. ○ Codes of conduct – not currently prevalent outside the GDPR, and not yet commonly used within it. Could become more so as codes are developed. ○ Certification – as with codes, a relatively new mechanism that it not prevalent, though could become more so. ○ Administrative arrangements between public bodies – not particularly prevalent outside the GDPR, but an important tool for public authorities. ○ Derogations – relatively common at national level, but by their		

			nature only to be applied in specific circumstances. ○ Authorisation from supervisory authority – while a small number of frameworks and national laws make provision for this in some circumstances, it is rare for all transfers to require authorisation. To do so may present barriers to data flows and a significant administrative burden on supervisory authorities.		
2.	**United Nations Conference on Trade and Development (UNCTAD)**	**Digital Economy Report 2021 – Cross border data flows and development: For whom the data flow.** **Published November 2021.**	The Digital Economy Report 2021 takes a deep dive into the development and policy implications of cross-border digital data flows to contribute to an enhanced understanding of these issues and aims to provide a "*fresh and holistic view of the development implications of this new kind of international economic flow*". **Trends in the data-driven digital economy**	The Report concluded that there is a clear need for global governance of cross-border data flows, complementing measures taken at other levels of governance. Currently, governance is based on a "*patchwork of national regulations with no satisfactory solution at regional or international level*", preventing the beneficial flow of data across borders.	Digital Economy Report 2021 (unctad.org)

			The Report begins by assessing recent trends in the data-driven digital economy, addressing issues relating to the definition and characteristics of data, an overview of recent developments in the data-driven digital economy in which cross-border data flows take place. The Report assesses the different types and uses of data, making the distinction between 'volunteered' data – provided by the user – and 'observed' data – extracted from activities on the web. The definition of data for the purposes of this Report is raw data – "observations that have been converted into a digital form that can be stored, transmitted or processed, and from which knowledge can be drawn" (Statistics Canada, 2019). International flows of these raw data are at present 'poorly regulated' at the global level. **Data flows are hard to measure but growing fast**	The Report provides some orientation on the way forward but does not seek to offer solutions, suggesting a global, broad policy approach could be taken: "*To truly work for the benefit of people and the planet, an international data governance framework should seek to enable gains from data flows to be equitably distributed within and between countries, while ensuring that risks and concerns are addressed*." The increased growth in data-driven digital technologies and the global data economy offer global opportunities but also increased risks and threats. These are arguably best addressed with international collaboration to develop a global policy approach to regulating cross-border data flows. An inclusive policy dialogue involving all actors, resulting in the creation of a new	

			The Report acknowledges that the unprecedented acceleration in the process of digital transformation and emerging digital technologies (such as data analytics, AI, IoT, cloud computing and Internet-based services) due to the COVID-19 pandemic, has driven the emergence of data as a key global strategic asset, not only for economic growth but also for human rights, peace and security – associated with virtually all the 2030 Sustainable Development Goals. "*Monthly global data traffic is expected to surge from 230 exabytes in 2020 to 780 exabytes by 2026*." Moreover, evidence shows that international bandwidth use increased dramatically during the pandemic and is geographically concentrated in two routes – between North America and Europe and between North America and Asia. According to the Report, cross-border data flows is most commonly measured	international body to focus on data-related governance with the aim of reframing and broadening the international policy debate and building multilateral consensus, thereby establishing a new path for digital and data governance. The Report suggests there is a need for innovative approaches to governing data and data flows to ensure more equitable distribution of gains and to address risks and harms and calls for **more detailed research on cross-border data flows and development**, focusing on the priorities for developing countries, including: • Developing the effective definition and measurement of data and cross-border data flows. • The development implications of cross-border data flows. • Focusing on the multi-dimensional nature of data.	

			in terms of volume – total used capacity of international Internet bandwidth, the amount of data flowing in terms of bytes. There is a lack of information, however, on both the direction of the flows, and the nature and quality of the data. **Data-driven digital economy characterised by large imbalances** There are large imbalances globally, particularly for developing countries. in terms of both the traditional digital divide between developed and developing countries but also a new dimension in connection with the "data value chain" – for value creation and capture, both raw data and the capability to process them into digital intelligence are needed. The role of data as an economic resource and the importance of cross-border data flows in the process have increased, characterised by major power imbalances and inequalities between and within countries.	• Assessment of cross-border data flow policies, and the pros and cons. The Report recommends that this new global approach to data governance and cross border data flows should address a number of key policy areas and priorities: • Developing a common understanding about definitions of key data-related concepts; • Establishing terms of access to data; • Strengthening the measurement of the value of data and cross-border data flows; • Dealing with data as a (global) public good; • Exploring emerging forms of data governance; • Agreeing on digital and data-related rights and principles; • Developing data-related standards; and	

			Developing countries in particular risk becoming mere providers of raw data to global digital platforms while paying for the digital intelligence obtained from their data. The Report assesses that data governance is critical to ensure that the benefits of cross-border data flows are equitably distributed. **Review of literature on cross-border data flows** The Report includes a review of the literature on cross-border data flows, concluding that: • There is a lack of common definitions on data and cross-border data flows, hampering measurement and governance consensus-building; • Few studies discuss the development implications of cross-border flows of different types and taxonomies of data ; and	• Increasing international cooperation related to platform governance, including with regard to competition policy and taxation in the digital economy. To oversee and regulate this global policy approach, it is suggested that the United Nations will need to play a central role, as the existing international body serving all global nations, including developing countries, building a multilateral, multistakeholder and multi-dimensional institution. Utilising its current involvement and engagement in relevant data-related work this can also help build effective links with civil society, academia and the private sector. *"To ensure the full involvement of all countries in shaping the ways in which data flows are governed at the global level, the United Nations will need to play a central role."*	

			• Literature focuses on the trade dimension neglecting the multi-dimensional character of data and is limited to studies from mainly anglophone countries. The Report outlines significant gaps in the literature on cross-border data flows and development, with few studies from the viewpoint of developing countries and defines the priorities for future research: • Working on definitions and the measurement of data and data flows. • Focusing on the development implications of cross-border data flows. • Stronger emphasis on the multi-dimensional nature of data. • More balanced assessment of cross-border data flow policies, and the pros and cons.	**Making data flow for the benefit of all requires bridging the divides** Key suggested areas for development to consider include: • Building the appropriate skill set in Governments, building capacity and increased participation in the global debate. • A flexible and complementary approach to designing and implementing any international framework. • International support for developing countries in particular to develop capacity and resource to effectively engage and benefit from the evolving data-driven digital economy. In the context of cross-border data flows, international support would focus on formulating:	

			The issues regarding the nature of data and the cross-border flow of data and development The complexities in the relationship between cross-border data flows and development are strongly linked to the particular nature of data. Moreover, the diversity of views regarding data value, digital sovereignty and market mechanisms hamper regulation and sustainable development. Opportunities for developing countries to capture the benefits of the data value chain could be realised by *"consideration of the key domains of data policymaking"*, such as data protection, capacity building and rules driving economic growth; *"the devil is in the detail"*, moving away from the extremes of data localization and free market forces. **Annex to Chapter III: the way data flows across borders**, looks in detail at the flow	1. Legal and regulatory frameworks. 2. National strategies for economic development gains whilst safeguarding security and human rights. 3. Awareness raising of data-related issues and development implications. 4. Ensuring developing countries have a place at the table and means to participate effectively. Annex 1 – Annex to Chapter II – Summary of literature review on cross-border data flows Annex II – Annex to Chapter V – List of regulations reviewed on cross-border data flows	

			of data routed through different local, regional and international networks indicating two main scenarios: Data flows can be assessed by the movement of individual data packets through a country, routed through a data centre, and forwarded to the ISP's own network infrastructure or exchanged with the network of another ISP at an Internet exchange point (IXP) – utilising physical entry and exit points for determining cross-border data flows. Alternatively, if focusing on the information (data) as a whole, once all data packets have been reassembled, as opposed to the individual data packets, there are only two physical location points to measure cross-border data flows, the client's ISP and the destination server ISPs. This chapter also references detail on routing via the Border Gateway Protocol (BGP) and tracing protocol. (Pages 94 -96).		

			Diverging digital and data governance approaches risk fragmenting the digital space This Report examines the diverging approaches to governing data and cross border data flows. The Report calls for a new path for digital and data governance in light of the current fragmented data landscape, advocating innovative approaches to governing data and data flows, particularly for developing countries, to ensure more equitable distribution of the gains and also to address the inherent risks and harms from emerging digital technologies. The review of national policies suggests varying approaches to governing data and cross-border data flows, dependant on the technological, economic, social, political, institutional and cultural conditions in each country.		

			The "*cybersovereignty model*" advocated by China and Russia, sharply contrasts to the US model of "*free flow of information"* based on technological leadership. The US data governance approach is based on the control of data by the private sector and expansion through private digital corporations. The EU data governance approach advocates control of data by individuals based on values, the GDPR specifically, regulatory leadership and partnerships providing a global model for data protection – as of 2018, 67 out of 120 countries outside of the European Union had adopted GDPR-like laws (Srikrishna Committee Report, 2018) – termed the "*Brussels effect*". Lastly, China's data governance approach is based on the control of data by the Government, and their Digital Silk Road initiative for strategic expansion.		

			The Report sets out that the current global context suggests: • A risk of fragmentation in the digital space and of the Internet. • Global digital platforms continue to expand their own data ecosystems. • Tensions increase among the major players, fostering a race for leadership in technological development to gain economic and strategic advantage. • Such a silo-oriented, data-drive digital economy would not benefit the interests of developing countries • An increase in data-driven fragmentation would hamper technological progress, reduce competition, enable oligopolistic market structures in different , and allow for more Government influence hampering collaboration across jurisdictions and restrict data flows.		

			The Report emphasises that for developing countries there is a need to carefully assess the positive value of these models of expansionist policies, such as the offers of improvement in infrastructure, connectivity or data-related regulations, against the cost of relinquishing their data to entities based in foreign countries, losing their ability to drive value from the data. **Holistic approach to the governance of cross-border data flows** The Report research indicates that international and regional approaches to regulate cross-border data flows are either too narrow, focusing only on aspects such as trade or privacy, or too limited geographically, as in the case of regional approaches. However, the Report affirms that regional approaches do provide a useful steppingstone towards global data governance, particularly where this		

			involves members at a similar level of digital development as opposed to those in which significant power imbalances emerge. The Report proposes to reframe and broaden the international policy debate with a view to building multilateral consensus, and the need for global governance of cross-border data flows to find the basis for a middle-ground solution, moving away from the extremes of strict data localization or fully free market data flows. New regulations also need to consider all dimensions of data, both economic and non-economic to address data flows in a holistic manner – taking into account human rights, national security, trade, competition, taxation and overall Internet governance. **Reasons for global governance of data and cross-border flows**		

			The Report highlights the rationale behind global governance of data and cross-border data flows: • Global data governance would help enable global data-sharing and develop public goods that could help address major global development challenges, such as poverty, health, hunger and climate change. • Technical coordination across borders – ideally at the global level – is essential to avoid further fragmentation of the Internet infrastructure and the digital space. • Global data governance becomes more important in light of the implementation of 5G and IoT, as well as the acceleration in digitization triggered by the COVID-19 pandemic. These trends broaden the scope for vast data collection and monetization globally. Without a coherent underlying global governance framework to create trust, this could		

			lead to a backlash in terms of data-sharing. It would also amplify already existing concerns over the lack of transparency in the data value chain, and over the unequal distribution of benefits from data. • The proliferation of national regulations on cross-border data flows creates uncertainty and elevates compliance costs, which can be particularly pernicious for micro and small enterprises, especially in developing countries. The interconnected nature and high degree of global interdependence in the data-driven digital economy means that national policies in this area have spill overs on other countries. • In the absence of global governance of digital platforms, self-regulation has led to market structures defined by platforms that predominantly benefit themselves, with various development and policy implications. The increasingly		

			global reach and influence of major platforms makes it even more difficult for any single country to address related policy challenges. • There is a need to develop a comprehensive and coherent assessment of the risks, vulnerabilities and outcomes of the business models of the digital platforms, in particular social media platforms, against a background of rising online harm at the global level. • A global approach to data governance is needed to prevent long-standing inequalities against developing countries from becoming amplified in the data-driven digital space. It is essential to ensure that their local knowledge, needs and viewpoints become adequately represented in global policy discussions. • Given the interdependencies and the interconnected character of the global architecture of the Internet, the future of cross-border data flows should not be		

			determined only by a small number of major countries. The Report recommends that a global approach to data governance and cross border data flows should address a number of key policy areas and priorities: • Developing a common understanding about definitions of key data-related concepts; • Establishing terms of access to data; • Strengthening the measurement of the value of data and cross-border data flows; • Dealing with data as a (global) public good; • Exploring emerging forms of data governance; • Agreeing on digital and data-related rights and principles; • Developing data-related standards; and		

			• Increasing international cooperation related to platform governance, including with regard to competition policy and taxation in the digital economy. **New Institutional setup** The Report suggests a new institutional set up to meet the global data governance challenge. A new global institutional framework to include a mix of multilateral, multistakeholder and multi-disciplinary engagement. The United Nations would be at the centre of this as the most inclusive international forum in terms of country representation, ensuring representation of developing countries, and being able to build on current initiatives relevant to data governance, research, consensus-building activities and technical cooperation work. This global organisation would also need to build effective links to ongoing		

			processes and initiatives led by civil society, academia and the private sector.		
3.	**The Organisation for Economic Co-operation and Development (OECD).**	**Mapping commonalities in regulatory approaches to cross-border data transfers: OECD Trade policy paper. Published May 2021.**	• Cross border data flows underpin today's digitalised, connected world, but have given rise to several concerns, including relating to privacy protection. (Also intellectual property protection, regulatory reach, competition, and industrial policy.) • A patchwork of rules has emerged, creating uncertainties for governments, firms and individuals with respect to the applicable rules in a given situation, making enforcement more complicated and difficult, and increasing the cost to firms of operating across markets. In practice, countries are using a range	• There is no single mechanism to enable 'data free flows with trust'. Governments pursue different, even multiple and complementary, approaches. • It is the prerogative of governments to establish the mix of instruments or mechanisms that best serve their policy objectives, but greater understanding, discussion and agreement on these instruments can be conducive to greater overall confidence and trust. • The paper provides observations / contribution to discussions by identifying commonalities and	Mapping commonalities in regulatory approaches to cross-border data transfers | OECD Trade Policy Papers | OECD Library (oecd-ilibrary.org)

			of mechanisms and instruments to enable cross border data transfers with 'trust' – including unilateral mechanisms, plurilateral arrangements and trade agreements. • The aim of the paper is to identify commonalities, complementarities and elements of convergence between the different instruments to support international dialogue and cooperation on more predictable and transparent combinations of data flows and 'trust'. • Unilateral mechanisms for safeguarding cross border transfers include pre-authorised safeguards (required public sector approvals, such as adequacy decisions) – these were more common. Open safeguards (where discretion is left to the private sector, such as	convergence rather than differences. These observations should be seen as initial building blocks – a modest but important first step in efforts to make iterative progress on an issue where there are significant international divisions, which supports continued dialogue in this area to help identify where efforts might be most fruitful.	

			accountability principles, private sector adequacy evaluations and contracts) were also widely used. • Plurilateral arrangements which aim to generate consensus around privacy and data protection, including in relation to cross border transfers, have also been widely adopted. Examples are the OECD Privacy Guidelines, APEC CBPRs and the Council of Europe Convention 108 and related instruments. The report found significant overlap of elements covered in existing domestic privacy and data protection regulation across a sample of OECD and emerging economies. This suggests a high degree of commonality in existing frameworks and provides common ground to build on to enable transfers.		

			• Trade agreements now often include provisions on data flows. Not all provisions have the same depth – only some include binding commitments on data flows, and of those almost all include exceptions allowing parties to restrict data flows to meet 'legitimate public policy objectives', and all couple data flow provisions with provisions on privacy or consumer protection frameworks. • The report also notes that standards and technology-driven initiatives such as ISO standards and privacy-enhancing technologies (PETs, such as cryptography and sandboxes) are increasingly being used by companies to protect and control access to data. • The report suggests that a global architecture is emerging, noting		

			commonalities, convergence and complementarity: ○ Commonality between and within instruments – all, whether unilateral, multilateral or trade agreements seem to agree the dual goals of safeguarding data and enabling its flow across borders. ○ Convergence is apparent in trade agreements which combine data flow provisions with those of privacy and consumer protection frameworks, and in the principles underpinning domestic privacy and data protection frameworks. ○ Complementarity – there is a high degree of this between instruments, where unilateral mechanisms draw from, and contribute to, plurilateral arrangements and trade agreements increasingly reference		

			plurilateral data protection arrangements along with their binding data flow provisions.		
4.	**World Economic Forum/ Bahrain Economic Development Board/Steering Committee-led project community of multistakeholder groups of businesses, civil society actors, academics and governments globally consulted on what makes cross-border data policy fit for**	**A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy.** **White Paper, published June 2020.**	• The ability to store, move and process data across borders is a foundation of the modern economy, with the focus on digital growth in the post-Covid-19 era. • Laws and policies that act as barriers (such as data localization) are on the rise, which could slow technological innovation. • The report 'debunks' several myths about data localization: ○ Data is not better protected by restricting it to one country – businesses prefer regulatory certainty.	• Proposes a practical Roadmap for governments, including country-level policy building blocks to harness the benefits and minimise the risks of cross border data sharing. • While it should be noted that it applies to non-personal as well as personal data, the roadmap for cross border data flows recommends: ○ Allow data to flow by default – prohibit data localization except in very specific circumstances. ○ Establish a level of data protection – national legal frameworks in place; cooperation mechanisms between authorities to allow for	WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf (weforum.org

	purpose and future-proof.		○ Data localization cannot effectively address privacy concerns, which instead need robust country-level data protection laws and controlled access to data, regardless of where it is stored. ○ Data localization does not improve data and cybersecurity. There are risks in storing data in one country. Instead, robust security controls are needed, not geographic locality requirements. ○ Data localization can compromise the ability to detect and monitor fraud, money laundering and terrorism financing activities, as criminals rejected in one country can attempt similar activities in another. • Certain regulatory differences between countries are necessary and appropriate; sovereign nations have	compliance across borders; adequacy agreements of other countries' data protection regimes. ○ Prioritize cybersecurity, in line with international norms, and maintain robust data security infrastructure. ○ Accountability between nations – establish cooperation mechanisms between national authorities to hold governments accountable for the security and confidentiality of the data they share. ○ Prioritize connectivity, technical standards to increase interoperability, facilitate data portability and encourage data publishers to ensure data integrity (data provenance). ○ Future-proof the policy environment, allowing for the possibility of future models such as data trusts.	

			different values and strategic priorities. • Core data protection principles remain fairly consistent between jurisdictions. When there are significant differences, barriers to cross border data flows can emerge. • Several cross border transfer mechanisms are mentioned, such as: ○ Adequacy arrangements (provides countries with opportunities for privacy law harmonization and bilateral trade negotiations) ○ Codes of conduct ○ BCRs ○ Consent ○ APEC CBPRs ○ Standard contractual clauses. While acknowledging that they are an important instrument, it is noted that SCCs are quite complex		

			and rigid but are often the least burdensome option for companies. The report also says that the requirement to pass SCC requirements to onward transfers multiplies costs and burdens for business, and that they are not ideal for cross-border sharing use cases such as machine learning. It is also noted that if every country imposes its own SCCs in the same vein as the EU then this will unduly burden companies and in turn trade. ○ Mutual recognition of, for example, OECD countries or signatories to Convention 108 is suggested as an alternative. • There is a clear need for interoperable policy frameworks, in order to create trust between nations when allowing companies within		

			them to participate in the international data economy. • This in turn allows for investment and economies of scale. • It was noted that core data protection principles can provide a place to start to achieve harmonization and interoperability, to reduce friction over cross border data flows.		
5.	**Information Technology and Innovation Foundation (ITIF) – a non-profit, nonpartisan research and educational institute, focusing on the intersection of technological**	**How Barriers to Cross-Border Data Flows are Spreading Globally. What they cost and how to address them.** **Report published July 2021.**	• Covid-19 made it clear that data flows are critical to the global economy – for both the economy and society. • Many countries have enacted barriers to data transfers that make them more expensive and time-consuming. The report notes an increase in data localization measures around the world, and says that this reduces trade and productivity. The report	• Policymakers should update laws to address legitimate data-related concerns, but should ensure that the benefits of data and digital technologies can also be maximized. • To build an open, rules-based and innovative digital economy, countries like Australia, Canada, Chile, Japan, Singapore, New Zealand, US and UK	https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

	innovation and public policy		even suggests that the GDPR's limited, complicated and uncertain mechanisms could lead to de facto localization. • Data localization makes the internet less accessible and secure, more costly and complicated, and less innovative. It undermines the potential for shared governance, which would otherwise allow countries to work together to address legitimate concerns about data transfers, such as to prevent espionage, maintain financial oversight, and to conduct law enforcement investigations. • The report praises Japan's putting data governance and localization on the global agenda vis the concept of 'data free flow with trust' – a vision where openness and trust exist in	must collaborate on constructive alternatives to data localization. • Governments should provide multiple mechanisms for the cross border transfer of personal data, accessible to firms of all sizes. Countries should explicitly mention acceptable frameworks and standards for transfers. • Governments should encourage firms to improve consumer trust through greater transparency about how they manage data, such as by regular disclosure about government requests for data. • Governments should support the development of global data-related standards, via multistakeholder and intergovernmental forums such as OECD.	

			symbiosis, not as contradictions. However it is noted that the concept has not yet been fully defined.	• Governments should provide more assistance to developing countries to help with digital economy policy. • Policymakers should focus on building interoperability between different regulatory systems – this is the most realistic goal for global data governance. Interoperability is described at several levels – with regulatory interoperability being built by governments through mutual recognition agreements between countries, recognising others' respective regulatory approvals or certifications as valid in their own country and explicitly referencing specific standards and legal frameworks such as APEC CBPR. • They should also make the APEC CBPRs a global model for data	

				governance by opening it up to non-APEC members – to focus on core principles and accountability rather than strict legal harmonisation. • Support efforts by like-minded, value-sharing democratic countries working together to develop a 'Geneva Convention for Data' to establish common principles, processes, and safeguards to govern government access to data. • Improve existing and build new mechanisms to improve cross border requests for data related to law enforcement investigations, such as CLOUD Act agreements and updated mutual legal assistance treaties, to provide timely assistance.	
Regionally-focused reports / papers					

6.	**United Nations Development Programme (UNDP) Global Centre for Technology, Innovation and Sustainable Development – a joint initiative by the Government of Singapore and the United Nations Development Programme (UNDP).**	**Enabling Cross-Border Data Flow: ASEAN and Beyond.** **Report published February 2021**	The paper discusses how to make cross-border data happen in terms of policies and processes; available mechanisms; and technical components. A. Policies and Processes a. With fragmented national requirements on the use of personal data in place (e.g. some Member States in favour of data localisation), ASEAN governments are struggling to strike a balance between facilitating digital economy through cross-border data flows and achieving privacy and national security goals. b. While data governance frameworks for accountable and transparent data processing help to protect rights of privacy, the improved compatibility of cross-border data transfer frameworks would enhance legal certainty,	A. A need to shape new models of data governance should be explored considering: a. the crucial role of data in economic and societal development; and b. the reality demanding engagement with the requirements of enabling cross-border data flows. B. ASEAN countries should contribute to enabling cross-border data flows which requires: a. national engagement with the realities of cross-border data from polices to technical architecture; b. shaping a strong regional data governance framework to boost potential from polices to technical approaches; c. avoiding protectionist approaches; d. ensuring continued convergence between national policies	Enabling Cross-Border Data Flow: ASEAN and Beyond | United Nations Development Programme (undp.org

			especially for private sector organisations. B. Cross-border Data Mechanisms a. The ASEAN framework on Digital Data Governance attempts to develop a regulatory framework in light of varying maturity levels and national laws among Member States, respecting digital sovereignty – one of its strategic priorities is to ensure business certainty and prevent unnecessary restrictions regarding cross-border data flows. b. The mechanism involves two fundamental methods of 'Certification' and 'Model Contractual Clauses,' while 'Binding Corporate Rules' and 'Codes of Conduct' are also	regarding data protection legislation; e. taking a forward-thinking approach to regulation in the context of a technology-driven sector; and f. investing in and enabling the considerable technical foundations required to enable cross-border data flows. C. The need for extensive industry engagement and the role of organisations are important, which includes: a. supporting coordination at an ASEAN level; b. building capacity and expertise; and c. driving collaboration and shaping best practices. D. These efforts should be founded on working closely with existing initiatives,	

			popular approaches to facilitate cross-border data flows. C. Technical Components a. Technical interoperability is crucial to facilitating cross-border data flows, ensuring data is shared between different systems and enabling those systems to make use of the data. b. Technical components necessary to ensure the safe transfer of data across borders and enhance interoperability between systems include connectivity, data standards, data sandboxes, data portability, encryption, etc. (Case Study) Open Banking as a business model based on the ideal of developing a single, cohesive pool of data that spans all financial products and services.	such as by aligning with the Working Group on Digital Data Governance.	

7.	**Asian Business Law Institute (ABLI).**	**Transferring Personal Data in Asia: A path to legal certainty and regional convergence.** **Comparative Review published May 2020**	-Review sets proposals for how Asian public stakeholders may promote legal certainty and consistency between their laws and regulations on transfers of data in Asia. Provides comparative overview and analysis of transfer principles mechanisms, legal grounds of region which will promote (i) legal certainty on transfer restrictions and (ii) help gain access to legal texts which is currently a burden; -There exist connecting points in national frameworks, despite the cultural differences, that regulators can work on to promote responsible data flows; -Most Asian DP laws contain provisions on data flows (some are currently working on this). However, this area still requires clarity and consistency in Asia. Need for interoperability is clear. - <u>Key findings:</u>	-**Consent:** Although legal harmonisation of consent criteria in Asia is illusory, convergence can be attained through other means: ✓ Lawmakers should not make consent compulsory (rather used in exceptional circumstances) and provide that other solutions can constitute an alternative legal basis. ✓ Coherence should be found in the conditions in which consent based transfers can take place. ✓ Adoption of "Privacy Codes" following dialogue between industry and regulators. -**Adequacy:** To ensure convergence: ✓ the most developed data protection law must be taken as a basis for the adequacy assessment;	Transferring-Personal-Data-in-Asia-A-Path-To-Legal-Certainty-And-Regional-Convergence-1.pdf (fpf.org)

			• **Collective benefits of legal certainty and convergence:** A unified set of data transfer mechanisms across Asia would (i) facilitate compliance by organisations to which multiple legal frameworks apply (avoidance of unnecessary duplication of compliance efforts, streamline accountability measures internally improving time and efforts, especially important for SMEs and start-ups) (ii) be in the interest of individuals (less effective regulatory oversight, resources otherwise used to improve data protection practices, increase public confidence in local and overseas dealings) • **Major areas of differences:** Rules on transfers (different approaches on restriction of data	✓ clear criteria of the assessment of adequacy must be defined. ✓ The absence of a regional body to coordinate the assessment creates a risk that different jurisdictions will draw contradictory conclusions. -**Self-assessment by the exporting organisation:** This assessment creates practical burden especially when the law does not list the standards for the assessment. It is also unrealistic due to the continuous changes on the ground but also due to inability to assess the practical implementation of the regime. ✓ If such assessment is to be recognised, clear guidance is required on how the assessment is to be done and who is qualified to do it. -**Contractual Safeguards:** Their enforceability as a binding legal instrument	

			flows), regulatory structures, Coverage of legal grounds, Implementation approaches. Differences are underpinned by fundamentally different logics. • **Potential for convergence**: in particular for interoperability of contracts, BCRs, certification and statutory exemptions. • **Convergence is achievable at multiple levels:** Ongoing law reform, implementation of regulations, issuance of ad hoc guidance, confirmation by regulators that specific tools can be read into general provisions of the law and instauration of a permanent effective pan-Asian coordination mechanism to follow developments and ensure consistency. • **Alignment on common standards:** Alignment of the	is certain under any national framework and their geographical reach is not limited. For convergence: ✓ Same set of contractual safeguards compatible within Asia and beyond with detailed clauses including on the recourse of individuals, through setting of contractual data privacy and security controls; ✓ Should allow for flexibility in implementation; ✓ Combination of contracts with other transfer mechanisms (e.g. BCRs, certification) could also be explored. -**BCRs**: Are now recognised as a valid transfer tool in several Asian DP laws therefore there could be interest in making them compatible in Asia and beyond. Lack of interest due to the administrative requirements under the European cooperation procedure.	

			assessment procedure and criteria of data transfers provisions • **Global standards:** Alignment to regional, sub-regional and global standards is necessary • **Guiding principles for data transfer mechanisms:** Any transfer mechanism must consist in a legally binding arrangement and must maintain existing privacy protections in national legislation, DS rights must remain enforceable overseas, adequate supervision must be in place. • **Consent:** Consent should not be made compulsory in all circumstances. All legal basis should be put on equal footing. Consent criteria, methods of obtaining consent should be coherent and provided in detail in	✓ Exploration of whether there is demand for this tool in Asia. -**Certification:** Possible to converge certification schemes so that an organisation can be certified under multiple Asian frameworks (or global in the future). Governments need to work on: ✓ The certification criteria to be approved by the regulatory authority; ✓ The determination of appropriate recourse mechanisms for individuals in case of breach overseas; ✓ The criteria for accreditation of certification bodies to ensure equality in independence; ✓ The identification of sufficient and clear benefits of certification; ✓ Avoidance of overlap and proliferation of certifications;	

			guidance following dialogue with stakeholders. • **Assessment of the level of protection in destination country:** Many DP laws subject data transfers to the assessment of the level of protection in the country of destination or the OECD Privacy guidelines with the adoption of "white lists". • **Contractual safeguards**: Contracts are the most widely used transfer mechanism in Asia and globally. Model clauses with guidance are proven very useful. • **BCRs:** Exploration of whether there is demand to use in Asia. • **Certification**: Japan, Singapore and South Korea already have such mechanisms in place. This mechanism would most likely provide convergence. Governments and regulators	✓ Enabling alignment of such schemes at global level. -**APEC CBPR:** They could benefit of network effect in Asia if more jurisdictions join. ✓ Need to clarify interrelationship with local laws, consider sectors and geography of the organisations operations; ✓ Non-APEC economies could adopt similar certifications that are interoperable with CBPR; ✓ CBPR could be globalised and opened-up for participation by all qualifying countries. -**Codes of Conduct:** Government and regulators need to work on: ✓ Setting conditions that such codes should implement to establish sufficient levels of protection for data leaving their jurisdictions;	

			need to work on different criteria (assessment, approval etc.) • **APEC CBPRs and PRP:** Important point for organisations is that CBPRs does not displace the domestic law of a participating economy. Therefore, can CBPR certification be useful to discharge at least data transfer requirements under multiple DP laws? Do the benefits outweigh the costs? • **Codes of Conduct:** Useful instruments to help organisations "tailor-make" general data protection provisions to their specific sector and needs. Advantages: ✓ Way of demonstrating compliance with nation laws to businesses, individuals and regulators;	✓ criteria of approval of Codes; ✓ conditions of legal bindingness in multiple jurisdictions; ✓ appropriate recourse mechanisms for individuals for breaches overseas; ✓ accreditation of monitoring body; ✓ identification of benefits to adhering to a Code; ✓ avoidance of overlap and proliferation of Codes; ✓ enable alignment of such schemes at global level; ✓ build on experience developed on Codes of Conduct (guidance issued by regional regulators e.g. Australia, Codes of Conduct work under the GDPR, lessons from specific industries e.g. cloud computing) -**Exemptions:** To ensure convergence there is need of harmonisation of:	

			✓ Competitive business advantage ✓ Adherence to global code would enable to discharge data transfer obligations. • **Exemptions:** Many of them take the form of statutory exemptions. Although prima facie national exemptions look similar in effect the vary significantly. • **Administrative exemptions:** Such exemptions are granted upon request in some jurisdictions. Convergence could be guaranteed if the rationale behind them could be transposed into their own frameworks subject to similar conditions. • **Data transfer requirements and localisation laws:** Several Asian jurisdictions have implemented or are considering to, so-called data localisation measures by which	✓ already existing neutral statutory exemptions (e.g. performance of a contract); ✓ the principle of their exceptional use; ✓ their use subject to a test of "reasonableness" ✓ the need to put in place appropriate safeguards for data privacy and security. ✓ The need of key obligations to still be complied with (e.g. transparency) **-Data transfer requirements and localisation laws:** To ensure convergence there is need of clarification of: ✓ scope and impact of such localisation measures; ✓ key concepts which underpin these laws (list of data covered by the law should be closed and defined;	

			organisations must store and /or process personal data generated within their territory even where specific data transfer mechanisms have been implemented. Therefore, data exports take place in derogation. This area of law is marked by uncertainty (constant changes in the past years). -The Review continues with a presentation of the legal framework on personal data in Asia and a comparative analysis of the different provisions. - The conclusions and recommendations of the Review following this analysis are presented in the next column.	✓ the circumstances in which exemptions are permitted; ✓ the regulatory expectations as to the practical consequences of localisation; ✓ interplay between transfer provisions in data protection laws and localisation obligations in specific sectoral laws or regulations. Also: ✓ Entry into force periods should be of significant duration; ✓ Consistent standards should be applied to localisation requirements in regulations applying to different sectors. **General recommendations and remarks for convergence:** ✓ Importance of ensuring that numerous mechanisms and legal	

				bases to frame data transfers should be included in any privacy law; ✓ There is need of maximum overlap between Asian legal systems regarding acceptable data transfer mechanisms and schemes; ✓ Implementation of these mechanisms and schemes should be subject to comparable conditions so that they can be used for compliance in multiple jurisdictions; ✓ Data protection frameworks should recognise the validity of specific transfer instruments by applying the same reading grid to all so that they provide the same safeguards; ✓ Same criteria should be shared across legal systems in order to	

				promote legal certainty, convergence and interoperability. Every transfer mechanism must: ✓ Consist in a legally binding arrangement; ✓ Maintain and build upon the existing privacy protections set out in national legislation and consistent with principles of international frameworks ✓ Data subject rights must be enforceable overseas; Adequate supervisory mechanisms for enforcement must exist.	
8.	**Milieu Consulting SRL, for the European Data Protection Board**	**Government access to data in third countries** **(Published November 2021)**	Reviewed public authority access to data and individual redress mechanisms under China, India and Russia DP Laws. The study presents the legal framework and practice in China, India and Russia on	The study reflects the data protection rules and safeguards provided in the legal system and practice of these 3 countries. At the same time, it highlights, in particular, the possibilities of access to data processed by the economic actors in these 3 countries for national security	Legal study on Government access to data in third countries | European Data Protection Board (europa.eu)

			their governments' access to personal data processed by economic operators. Covered various applicable laws or laws with Privacy elements (including constitution, cybercrime, law enforcement, etc) laws in each country. The information and research was done through a variety of resources, comprised of interviews with in-country legal practitioners, scholars, and other knowledgeable persons.	purposes, the exemptions to data protection in this regard, the (non-) existence of avenues for redress. While no formal conclusion is drawn in this study, it provides factual elements to be used when analysing the 3 legal frameworks and practices in these countries. General conclusions for each, for similar reasons mainly around human rights policy failings, or broad use of "national security" as an exemption or legal basis for obtaining data and / or preventing redress, were that each country lacked effective safeguards for foreigners' data protection. As a result, generally for each country, transferring data to them would be high risk to individuals and the exercise of their rights when data is unlawfully or unfairly processed by controllers or processes based in them.	

				With respect to the work of this group, a recommendation may be to refine cross border rules based primarily on how companies implement the laws, what tools and shields should "attach" to personal data when it is transferred to similar jurisdictions, and what the main risks are based on a risk index.	
9.	**University of Cambridge Faculty of Law** **(Christopher Kuner)**	**Legal Studies Research Paper No: 20/2021** **Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection** **(Published April 2021)**	- In recent years concern has grown about threats to the data protection rights of EU individuals originating from outside the EU. - EU data protection law **has two main weapons** in its armoury to protect against such threats, namely rules concerning the **territorial scope** of data protection law, and restrictions on **international data transfers**: 1) The first set of rules determines the conditions under which EU data protection law applies outside EU		Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection by Christopher Kuner :: SSRN

			borders, and will be referred to here as territorial scope rules 2) The second set of rules restricts the transfer of personal data outside the EU, and will be referred to as data transfer rules. - For the protection of EU data against external threats to be both legally sound and effective in practice, it is **necessary to examine the nature and interaction of rules on territorial scope and data transfers**, in order to determine how the EU's vision of cross-border data protection can be realised. - In recent years, **initiatives have been proposed by the EDPB and the European Commission to address the interaction of territorial scope and data transfer rules**: The initiatives (EDPB, ICO) all **place territorial scope rules over data**		

			transfer restrictions by disapplying such restrictions in cases where the law already applies to data processing abroad. They are also implemented in a variety of ways, from non-binding but influential guidance from DPAs, to a proposed Commission decision, to changes to national privacy legislation. Third countries are also interested the topic, so that the EU's approach to this question will have impact abroad, particularly in those countries whose data protection systems are tied to those of the EU. - **Evaluating Territorial Scope and Data Transfer Rules:** There are important differences between the rules of Article 3 and Chapter V, and that more explanation is needed before action is taken to disapply one of them. While they could undoubtedly be better harmonized		

			in order to enhance legal clarity, this could be achieved better through other mechanisms than through the disapplication of data transfer rules. - **Towards better protection of cross-border data processing :** The tension between territorial scope and data transfer rules reflects the difficulty of providing seamless global protection for data processing. The authors of the paper suggest several options: 1) a clause could be inserted in Article 3 to clarify their relationship. 2) combine obligations under Article 3 and Chapter V with regard to parties in third countries that both interact with EU individuals and receive data transfers from the EU.		

10.	**European Data Protection Supervisor**	**Case Law Digest 2021: Transfers of personal data to third countries** **(Published June 2021)**	• "The overarching principle of 'the law of transfers' is the continuity of protection of personal data, and in so doing of the protection of fundamental rights and freedoms of the individual. Being a fundamental right, data protection concerns everyone in the Union, and wherever her or his personal data goes, even when data 'travels' to a third country." • The digest provides summaries of significant case law relating to transfers of personal data to third countries, to clarify the structure of the analysis carried out by the CJEU in those judgments: ○ Lindqvist, 6 November 2003 ○ Schrems, 6 October 2015 ○ EU-Canada PNR Agreement, 26 July 2017 ○ Schrems II, 16 July 2020		Case Law Digest 2021: Transfers of personal data to third countries | European Data Protection Supervisor (europa.eu)

			• The digest also explores key issues relating to transfers by asking several questions and then providing relevant paragraphs of CJEU judgments in reply. Amongst others, questions relating to the following are included: ○ When a transfer to a third country takes place. ○ Powers available to national supervisory authorities in respect of transfers. ○ What is meant by an adequate level of protection. ○ What is meant by transfers of personal data as interference. ○ When, and subject to which conditions, have SCCs been considered a valid transfer tool by the CJEU. ○ What is meant by effective judicial and administrative redress.		

			○ What is meant by the duty to notify to the data subject the transfer of personal data. ○ Are specific safeguards needed in case of transfer of personal data subject to automated processing or involving sensitive data. ○ What are the data protection requirements in case of onward transfers of personal data.		
11.	**United Nations General Assembly: Human Rights Council**	**Report of the Special Rapporteur on the right to privacy, Ana Brian Nougreres - Privacy and personal data protection in Ibero-America: a step towards globalization?**	Not all content is directly relevant to cross border transfers, but several points are of relevance, as follows: • Notes the impact of the EU GDPR. Argentina and Uruguay have both adopted European-style models and have EU adequacy status, and that this has contributed to other Ibero-American states passing laws based on the European system. Lists Colombia, Costa Rica, Mexico, Nicaragua and Peru having adopted a	Suggests that the Ibero-American data protection system could provide a model for a way of working collaboratively towards a world where the principles of privacy and personal data protection are mutually agreed upon and respected, leading to the implementation of digital privacy standards, and where integration and harmonization are goals that can be achieved without departing from the ethical principles that guarantee respect for human diversity.	OHCHR | A/HRC/49/55 : Privacy and personal data protection in Ibero-America: A step towards globalization? - Report of the Special Rapporteur on the right to privacy

			similar model before the Ibero-American network developed its standards. Laws passed recently also broadly follow the GDPR's general outline, in Brazil (2018), Panama (2019) and Ecuador (2021). • Emphasises the importance of integration and harmonisation as attainable goals.		

GPA GFSWG Literature Review: Articles/Blogs/Announcements on Cross-Border Data Flows and Transfer Mechanisms

No.	Organisation	Title	Main points / views	Link
General articles / blogs / announcements				
12.	**IAPP (US contributor)**	**Doing business across borders – a global future or a splintered internet?** **Article, published January 2022**	-2000 Yahoo case already set precedent in which a country (France) has the right to reach its physical boundaries to impose rules on data stored in other nations; -Governments increasingly pass laws with extraterritorial reach (e.g. GDRP or Chinese DP law) under which if there is a physical transfer of data transfer tools must be put in place; - Consequences: (i) customer loss due to difficult compliance regimes and strict rules (e.g. EU) and (ii) rise of data nationalism especially due to Schrems II. Proof are recent decisions of EU DPAs (Portugal, Austria, Germany, Netherlands) and EDPS suspending transfers or use of Google Analytics in Europe. Also, China leans towards data nationalist measures with PIPL, recent cyber	Doing business across borders — A global future or a splintered internet? (iapp.org)

			security law, and draft measures for data transfers; - SCCs are feared due to US surveillance but maybe the real reason is economic protectionism. -Difference between civil law (EU, China) where courts look at laws at hand and common law systems (UK) in which courts look at precedent; -Worldwide approach towards increased protectionist measures (Mexico, Brazil, India etc.) including in digital trade which lead to local businesses unwilling to share information due to uncertainty of privacy rules; - Future: Need for a global village, some efforts are still taking place to robust multinational agreements allowing for practical mechanisms for transfers, negotiations to put in place new EU-US agreement, US pursuing a digital trade agreement through the APEC.	

13.	**Diginomica Ltd**	**Data must flow in the digital economy, but the UN and Salesforce have issued separate warnings that there's a problem here.** **Article, published October 2021**	-Increased need for free flow but G20 leaning toward more restrictive data protection regimes; - UN: we need a holistic global policy approach that encompasses different types of data and balances interests and needs of involved countries with engagement of multistakeholder and multidisciplinary engagement. This approach must be flexible and needs to complement and be coherent with national policies. Global debates on cross border flows should be held under the auspices of the UN; (I) UNCTAD Digital Report 2021: - Existing frameworks do not address needs of global data governance; -Global framework is needed for (i) cross-border data flows and development of public goods, (ii) avoid fragmentation of internet infrastructure through technical coordination and increase trust; Key findings:	Data must flow in the digital economy, but the UN and Salesforce have issued separate warnings that there's a problem here... (diginomica.com)

			• Data flows are hard to measure but growing fast (US and China dominate data driven digital economy) • No common understanding of what data flows are and what they can empower (territoriality and national sovereignty assigned to data flows is a challenge) • Diverging approaches to governing data and cross-border data flows (US: control of data by the private sector, China: control of data by government, EU: control of data by individuals) This divergence creates tensions. (II) Salesforce White Paper Cross Border Data Flows Index (quantitative measure of G20 approach to data flows): - Data regulations across G20 economies are becoming more restrictive with data sovereignty on the rise. Consequence: more compliance and complexity with extra costs for businesses and less trust and transparency across governments.	

			-Japan and UK more open approach (UK risks EU adequacy), EU criticised for growing digital sovereignty, India, China and Russia very strict regulations on data transfers; -Recommendations: • Promote convergence and interoperability in privacy laws based in international standards (OECD Principles or APEC framework) • Expand agreements for access to information and government access • Create trusted data sharing frameworks with data protection and cybersecurity provisions • Encourage innovation Enable government policies for public and private sector enabling free flow.	
14.	**IBM**	**The future of cross-border data flows must include high standards of protection.**	-Companies and governments should encourage the free flow of data especially now with COVID while ensuring high standards of privacy and security;	The future of cross-border data flows must include high standards of protection - THINKPolicy Blog (ibm.com)

		ThinkPolicy Blog published December 2020	-Enhanced cooperation between countries can promote transparency and enhance public trust in the technologies that are essential today. Industries have to set high security and privacy standards guaranteeing adequate level of protection; -IBM measures to ensure security of data: • Encryption technologies when data are in transit, at rest or in use (Confidential computing, homomorphic encryption, quantum safe encryption) Does not voluntarily share data with governments requesting access to IBM clients' data rather asks governments to contact clients directly (following Schrems II and EDPB recommendations, IBM incorporates data policy on government access directly into contracts)	
15.	**Invest in Bahrain**	**Why cross-border data flows are essential in the post-Covid era.** **Article published October 2020**	Focused on tech policy around data flows, especially in long term emergency situations like a pandemic: - Covid pandemic revealed need for increased digitisation and for a regulatory framework	Why cross-border data flows are essential in the post-COVID era - Invest in Bahrain (koohejisystems.com)

			providing basis for economies to have compatible systems that ensure tech-based collaboration; - Right legislative frameworks need to be interoperable so that regions can streamline requirements and create mechanisms to reduce regulatory overload. It discussed the Bahrain / World Economic Forum partnership that launched a Roadmap for Cross-Border Data Flows. This is a regulatory framework providing the building blocks for major economies across the globe to roll out compatible systems that drive tech-based collaboration in order to enjoy the benefits and limit the risks of cross border data sharing. Roadmap includes recommendations for nations to develop best practice legislation. - Bahrain already has a robust data protection legislation but its interest for the project stems from the introduction of national policy frameworks to facilitate data flow allowing foreign governments to maintain their	

			jurisdictions over data stored in Bahrain- based data centres.	

16.	**US Department of Commerce**
	
	(Also Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei)
		Global Cross-Border Privacy Rules Declaration
		
		(April 2022)
			• A Declaration by Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America, as current economies participating in the APEC CBPR System to establish a Global CBPR Forum to:
			  ○ Promote interoperability and help bridge different regulatory approaches to data protection and privacy
			  ○ Objectives include establishing an international certification system based on the APEC Cross Border Privacy Rules, and to promote interoperability with other data protection and privacy frameworks.
			
			Activity will include promoting uptake of the Global CBPR and PRP Systems globally to facilitate data protection and free flow of data, with participation open to those jurisdictions
				Global Cross-Border Privacy Rules Declaration | U.S. Department of Commerce

			which accept the objectives and principles of the Global CBPR Forum.	
17.	**G7**	**Ministerial Declaration – G7 Digital Ministers' meeting, 11 May 2022** **Annex 1: G7 Action Plan for Promoting Data Free Flow with Trust**	The Declaration sets out (among other items) that the G7 will strengthen efforts to further common understanding and to work towards identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data free flow with trust, in order to foster future interoperability. Annex 1 to the Declaration, an Action Plan for Promoting Data Free Flow with Trust, includes plans to: • Strengthen the evidence base for DFFT – including understanding the opportunities and challenges of cross border data flows, existing regulatory approaches and instruments, better understanding of localisation measures and their potential implications and alternatives.	g7-praesidentschaft-final-declaration.pdf (bmvi.de) g7-praesidentschaft-final-declaration-annex-1.pdf (bmvi.de)

			• Build on commonalities to foster future interoperability (which might include further analysis of practices such as SCCs, and potential technologies to enhance trust). Also continued support of the OECD work on government access. • Continue regulatory cooperation, including through dedicated roundtables, possibly on regulatory approaches related to privacy-enhancing page 2 technologies (PETs), data intermediaries, web tracking, emergent risks, cross-border sandboxes, the promotion of interoperability of data protection frameworks, the OECD work on trusted government access, and the Global Privacy Assembly October 2021 Resolution on Government access to personal data. • Promote DFFT in the context of digital trade. • Share knowledge about the prospects for international data spaces.	
Regionally-focused articles / blogs / announcements				

18.	**The Register**	**UK and USA seek new world order for cross-border data sharing and privacy .** **Article published December 2021**	-US/UK to shape together new world for data sharing across borders; -US/UK share commitment to deepen data partnership including on adequacy and promote trustworthy use and exchange of data by designing and delivering next generation tools; - Ecosystem that promotes interoperability between data protection frameworks, facilitating cross-border data flows while maintaining high standards of data protection and trust; - US/UK looking forward to working with likeminded partners (including OECD) to build trust in government access for purposes of national security, law enforcement investigations and public safety; - US/UK partnering to overcome technical challenges related to privacy-enhancing technology. -UK secretary signed three digital trade-related (MOUs) with Singapore at the Future Tech Forum. At the Forum the UK also presented the UK's new Digital Trade Network, a three-year	UK and US officials meet to discuss cross border data flows • The Register

			pilot programme designed to support UK business wanting to grow digitally into Asia-Pacific;	
19.	**Gov.uk**	**UK – US joint statement on deepening the data partnership.** **Statement published December 2021**	- US/UK share commitment to deepen data partnership including on adequacy and promote trustworthy use and exchange of data; - US/UK key players in shaping global data ecosystem that promotes interoperability between data protection frameworks and facilitating data flows while maintaining high protection and trust by designing tools for 21st century; - US/UK looking forward to working with like minded partners to build trust in government access for purposes of national security, law enforcement investigations and public safety; - US/UK recognise the negative trends that risk closing off international data flows.	UK – US joint statement on deepening the data partnership - GOV.UK (www.gov.uk)

20.	**One Trust DataGuidance**	**China – Data Protection Overview**	Section 7.2, Data transfers: Summarises China's PIPL requirements for cross-border transfers of personal information, as follows: • Notes that PIPL provides three methods for cross-border transfers: ○ Critical Information Infrastructure (CII) operators and personal information handlers that process personal information beyond the to-be-determined threshold prescribed by the Cyberspace Administration of China (CAC) are subject to data localization requirements. Where transfers are necessary, exporting entities must pass a mandatory CAC security assessment. • For non-CII operators or personal information handlers processing below the threshold amount or personal information, two other options are provided:	China - Data Protection Overview | Guidance Note | DataGuidance

			○ Certification awarded by a recognised institution in accordance with regulations to be published by the CAC. ○ Data transfer agreement with the recipient, in compliance with CAC's standard contract. The author suggests this option is most likely to be used. • Additional requirements noted are: ○ Individuals must be informed of various details about the transfer. ○ Consent must be obtained. Cross-border transfers of personal information made for the purpose of providing international judicial and law enforcement assistance must first be approved by a competent Chinese authority.	
21.	**Cooley.com** **cyber / data / privacy / insights blog**	**Cross-Border Data Transfers: Part 1: PIPL vs GDPR vs CCPA** **(April 2022)**	• Notes that PIPL parallels the GDPR in various aspects relating to cross border transfers. • Like GDPR, PIPL requires a transfer mechanism - though it provides fewer mechanisms than GDPR.	Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA – cyber/data/privacy insights (cooley.com)

			• A difference is that PIPL imposes different obligations based on organisations' status (i.e. Whether the organisation is a 'critical information infrastructure operator') and the amount of personal information processed:
			  ○ CII operators and those processing personal information over the threshold provided by the CAC must locally store personal information collected and generated within China.
			  ○ Where they need to transfer data abroad, they must pass a CAC-administered security assessment.
			• Other mechanisms:
			  ○ If China is party to an international agreement containing relevant provisions on providing personal information outside China's borders, those provisions may be carried out. Authors not aware of any at the time of writing.
			  ○ Certification from professional institutions in accordance with rules adopted by the CAC. (No professional institutions accredited yet; rules	

			according to which certifications may be issued not yet adopted.) ○ Standard contract (first draft expected from the CAC soon) • Remains to be seen which mechanisms will be the most-used, and what the finalised versions of drafts will look like.	
22.	**Cooley.com** **cyber / data / privacy / insights blog**	**Cross-Border Data Transfers: Part 2: PIPL and GDPR Compliance Obligations on Cross-Border Transfers of Personal Information** **(April 2022)**	• Notes that, like GDPR, PIPL has additional compliance requirements: ○ Information requirements (ie informing data subjects of various details of the transfer) ○ Obtaining data subject consent in certain circumstances. ○ Carrying out an impact assessment prior to the transfer. ○ Ensuring the proposed recipient is not on a list issued by the CAC of those who conduct personal information processing activities that infringe Chinese citizens' rights and interests related to personal information and to whom transfers are restricted or prohibited. At the time of	Part 2: PIPL and GDPR Compliance Obligations on Cross-Border Transfers of Personal Information – cyber/data/privacy insights (cooley.com)

			the blog's publication, the CAC was yet to publish such a list.	
23.	**Cooley.com** **cyber / data / privacy / insights blog**	**Cross-Border Data Transfers: Part 3: PIPL's Localization Requirements and Restrictions on Responding to Foreign Judicial and Enforcement Agencies** **(May 2022)**	• PIPL requires that operators of critical information infrastructure and personal information processors who process a volume of personal information over a threshold specified by the CAC must store locally any personal information collected and generated in China. They can then only export that data when necessary and after passing a CAC security assessment. • Sectoral regulations may also impose localization requirements on specific sectors. • PIPL also introduces a 'blocking statute' that restricts personal information processors from providing personal information stored within China to foreign judicial or enforcement agencies - processors need the approval of a competent Chinese authority before they are allowed to respond to such requests. This could conflict with US laws such as the CLOUD Act, and it remains to be	Part 3: PIPL's Localization Requirements and Restrictions on Responding to Foreign Judicial and Enforcement Agencies – cyber/data/privacy insights (cooley.com)

			seen how these seemingly disparate requirements would be enforced.	

24.	**IAPP**	**IAPP The Privacy Advisor: Top 5 operational impacts of China's PIPL – Part 5: International Data Transfers**	• China's PIPL is still being fleshed out by implementing regulations and official guidance. It provides a regulatory framework that governs cross border transfers.
			• Other relevant legislation also exists: China's Cybersecurity Law and Data Security Law regulate the cross border transfer of "important data"
			• Notes that in general, a processing entity that plans to transfer personal information out of China needs to:
			  ○ Provide individuals with certain specific information and obtain separate consent (though notes that the exact requirements around consent are unclear).
			  ○ Adopt necessary measures to ensure overseas recipients provide the same level of protection as required under the PIPL.
				Top 5 operational impacts of China's PIPL — Part 5: International data transfers (iapp.org)

			○ Carry out a personal information impact assessment. • Notes that there are three transfer mechanisms on top of the general requirements: ○ Security assessment administered by the Cyberspace Administration of China (CAC) (for Critical Information Infrastructure operators and those processing a large volume of personal information (exact threshold is to be finalised) ○ Standard contractual clauses stipulated by CAC ○ Certification in accordance with CAC-specified rules. • On the above mechanisms, detailed rules/guidance is yet to be released, so the situation should be monitored.	
25.	**One Trust DataGuidance**	**India – Data Protection Overview**	Section 7.2, data transfers	India - Data Protection Overview | Guidance Note | DataGuidance

			• Notes that all companies involved in the payments sector must process and store all financial information in India. Payment transactions may be processed abroad but once completed, all data in relation to the processing should be stored in India and all records outside India should be deleted.
			• Subject to localisation requirements, the new Personal Data Protection Bill permits sensitive personal data to be transferred out of India in certain cases, for example if:
			  ○ In accordance with contractual clauses or intra-group schemes authorised by the DPA;
			  ○ It is made to a country, or a sector, or an international organisation approved by the government;
			  ○ The transfer is necessary (and the DPA has approved the necessity)
			  ○ In addition to one of the above three, explicit consent is obtained (currently unclear)	

			• The Bill is silent on the cross-border transfer of personal data that is not sensitive data. It is possible that the law does not intend to regulate such transfers over and above general processing requirements.	

GPA GFSWG Literature Review: Mechanism Development and Examples of Guidance on Cross-Border Data Flows and Transfer Mechanisms

No.	Organisation	Title	Main points / views	Link
26.	**Information Commissioner's Office, UK**	**International data transfer agreement and guidance** **(Published February 2022)**	• The UK's international data transfer agreement (IDTA), international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and transitional provisions came into force in the UK on 21 March 2022.	International data transfer agreement and guidance | ICO

			• The IDTA and Addendum replace the previous standard contractual clauses for international, transfers, and take into account the binding judgment of the European Court of Justice in the “Schrems II” case. • The IDTA or Addendum can now be used by data exporters as a transfer tool to transfer personal data outside of the UK in compliance with Article 46 of the UK GDPR. • When entered into as a legally binding contract, the UK Information Commissioner considers that the IDTA and the Addendum provide Appropriate Safeguards for Restricted Transfers. • Further guidance will be published by the ICO soon – on how to use the IDTA; clause by clause guidance on the IDTA and Addendum; guidance on transfer risk assessments; and	

			further clarifications on ICO international transfers guidance.	
27.	**FDPIC Switzerland**	**Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection.** **(Published September 2020)**	The FDPIC maintains a list of countries documenting the adequacy of data protection, he takes the following into consideration: 1. Legislation and its practical application by the individual countries and how this legislation is assessed by academia and courts; 2. Conventions, publications, official statements and decisions by domestic and foreign institutions and authorities on the equivalence or adequacy. As a result of a large number of country decisions on the adequacy of data protection, Switzerland, together with the EU, the EEA, and some non-European countries, now belongs to a group of nations which mutually assume the existence of an equivalent and adequate level of data protection.	See attachment 18

			A mutual need for coordination arises in particular when the adequacy of a third country has been reassessed, as it is currently the case in the EU/EEA member states following the latest ruling by the CJEU with regard to the USA. **USA and CJEU ruling on Schrems II** As Switzerland is not a member of the EU, it is not legally bound by the CJEU ruling. There is currently no legal decision in Switzerland comparable to the CJEU ruling. In view of this situation, the FDPIC had to reassess the position of the US on the list, but also to provide more detailed legal justification for any amendment to it: **Principles of lawful data processing according to FADP is violated:** • for persons concerned in Switzerland there is **no enforceable legal remedy** with regard to the data access by US authorities, especially since the effectiveness of the ombudsperson mechanism, which is intended to guarantee an indirectly	

			enforceable legal remedy, cannot be assessed due to a lack of transparency; • that the decision-making powers of the ombudsperson vis-à-vis the US intelligence services and its actual independence cannot be assessed owing to a lack of clear and conclusive information. As a result of this assessment based on Swiss law, the FDPIC concluded that **the indication 'Adequate level of protection under certain circumstances' had to be removed for the US in the FDPIC's list of countries.** Contractual safeguards such as the EU's SCCs, which are also frequently used in Switzerland, or so-called BCR cannot prevent foreign authorities from accessing personal data if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency and legal protection of the persons concerned. **Ends with Practical advice for Swiss companies transferring data to non-adequate countries.**	

28.	**FDPIC Switzerland**	**A guide to checking the admissibility of direct or indirect data transfers to foreign countries** **(Published June 2021)**	This guide is intended to make it easier for data owners to check the permissibility of transfers of personal data abroad. Based on a flow chart, this guide explains how Article 6 paragraph 2 letter a FADP applies if the foreign country concerned does not have legislation that ensures adequate protection and sufficient safeguards. If the country is not on the FDPIC's list of countries that offer adequate data protection or if, despite its presence on the list of countries, there are indications that an adequate level of data protection cannot be assumed for the intended export**, the data exporter must ensure data protection by introducing sufficient safeguards, in particular by means of a contract.** As a rule, **Standard Contractual Clauses (SCCs)** will be used as a basis. It should be noted that internal company data protection regulations, so-called **Binding Corporate Rules (BCR)**, which regulate the cross-border transfer of data within a group of companies or between different companies under uniform management, cannot be used by a data exporter in an external relationship as a substitute for SCCs.	See attachment 19

			The data exporter must keep detailed records of the data transfer, e.g., by means of a directory; these records form the basis for assessing the intended data export With regard to official access in the third country (e.g. for national security or criminal investigation purposes) and the rights of the data subjects, the data exporter must check whether such access and rights are compatible with Swiss data protection law and Swiss constitutional principles. **4 Rights** equivalent to the following Swiss fundamental **rights must be guaranteed** in the third country: 1. **Principle of legality:** clear, precise and accessible rules 2. **Proportionality** of the powers and measures regarding the regulatory objectives pursued 3. **Effective legal remedies** must be available to the individual	

			4. **Guarantee of legal recourse and access to an independent and impartial court** If the four guarantees are given, an adequate level of data protection can be achieved with standard SCCs. If the guarantees mentioned are not comprehensively given in the third country, additional measures that serve as "substitutes" for the missing four guarantees must be examined in advance in each case, ex. Additional contractual measures, additional technical and organisational measures, If additional measures cannot compensate for the identified deficiencies in fulfilling the four guarantees and that there is therefore no sufficient guarantee, the data transfer abroad must be suspended or terminated immediately. An annex helps to do the assessment.	

29.	**European Union**	**Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries** **(Published June 2021)**	To help controller and processor be in line with art 46(1) of Regulation (EU) 2016/679, the Commission provides standard contractual clauses that can be used to facilitate the transfer of personal data from a data controller, established in the European Union, to a controller or processor established in a third country that does not offer an adequate level of protection. The Commission provides a general template of standard contractual clauses that combines general clauses and specific clauses with a modular approach, to capture the various transfer scenarios (transfer from controller to controller, from controller to processor, from processor to processor, from processor to controller). Thus, controller and processor should select the module applicable to their own situation by considering: - their respective position in the transfer (data exporter or data importer), the content, the duration of the contract, the	See attachment 20

			nature of the data to be transferred, the type of recipient, the purpose of the processing, the storage limitation, transparency requirements, the accuracy and minimisation of the transferred data or the security measures under consideration. - the laws and practices of the third country of destination, and in particular the validity of contractual clauses under national laws or the data importer obligations in a case where local public authorities access the transferred data. Moreover, controllers and processors should agree on additional safeguards to ensure a level of protection essentially equivalent to that guaranteed within the Regulation (EU) 2016/679, when the abovementioned standard contractual clauses are not sufficient. Such additional safeguards could be contractual, technical and/or organisational measures that will apply to any transmission of personal data and its processing.	

			To conclude, Standard Contractual Clauses is a useful tool to set up a minimum standard of data protection requirements for cross-border transfers. This legal tool eases international data transfers, despite different national legislations.	
30.	**Article 29 Data Protection Working Party**	**Working document setting up a table with the elements and principles to be found in Binding Corporate Rules** **(Revised February 2018)**	The former Article 29 Working Party (replaced by the EDPB) sets up a table with the elements and principles that should be found in Binding Corporate Rules in order to reflect the requirements expressly set out by EU Regulation 2016/679. There are two different kinds of BCR : - BCR-Controllers (BCR-C) are suitable for transfers of personal data from Controllers established in the EU to other Controllers or to Processors (established outside the EU) within the same corporate group; - BCR-Processors (BCR-P) apply to data received from a Controller (established in the EU) which is not a member of the group, and then processed by the group	See attachment 21

			members as Processors and/or Sub-processors. The Working Document sets up a table that intends to clarify the necessary contents of BCRs as stated in Article 47 of Regulation (EU) 2016/679. The BCR, among others: - must be legally binding and shall contain clear duties for each participating member of the Group; They should explicitly include the following principles to be observed by the company: transparency, fairness and lawfulness; purpose limitation; data minimisation and accuracy; limited storage periods; processing of special categories of personal data; security; restriction on transfers and on onward transfers to processors and controllers which are not part of the group; - must expressly confer rights to data subjects as third-party beneficiaries, such	

			as data protection principles, rights of access (e.g. rectification, erasure, restriction, objection to processing…), the right to judicial remedies and the right to obtain redress; - must contain the duty for one of the European members of the Group to accept responsibility for and to agree to take the necessary action to remedy actions of other members outside of the EU bound by the BCRs; - must contain the commitment that all data subjects should be provided with the information required by Articles 13 and 14 of Regulation (EU) 2016/679; - must set up an internal complaint handling process to ensure that any data subject should be able to exercise his/her rights and should be able to complain about any actions taken by any member subject to BCR; - must state that an appropriate training should be established for personnel that	

			have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data; - must create a duty for the group to have data protection audits on a regular basis or whenever the Privacy Officer requires it, to ensure compliance with the BCRs; - should create a network of data protection officers (DPO) or appropriate staff for monitoring compliance with data protection rules. - should contain a commitment that when a member of the corporate group is subject to a third country law that has a substantial adverse effect on the guarantees provided by the BCRs, the problem will be reported to the competent supervisory authority (unless otherwise prohibited, such as an obligation under criminal law to preserve the confidentiality of a law enforcement investigation). This includes any legally	

			binding request for disclosure of personal data by a law enforcement authority or state security body. To conclude, BCRs provide a useful tool to ensure compliance of international data transfers inside a group of enterprises, by defining a minimum level of data protection requirements regardless of the localisation of the enterprises in the word.	
31.	**European Data Protection Supervisor**	**Strategy for EU institutions to comply with "Schrems II" Ruling** **(Published October 2020)**	• This strategy was published in October 2020 and aimed to ensure and monitor compliance of EU institutions (EUIs) with the Schrems II judgment. • In the short term, EUIs were ordered to map and identify which ongoing contracts, procurement procedures and other types of cooperation involved transfers of data, and to report to EDPS any transfers without legal basis, transfers based on derogations and transfers to private entities towards the US. EUIs were also strongly encouraged to avoid	Strategy for EU institutions to comply with "Schrems II" Ruling | European Data Protection Supervisor (europa.eu)

			new processing activities involving transfers of personal data to the US. • In the medium term, EUIs were asked to carry out case-by-case Transfer Impact Assessments, to identify whether an essentially equivalent level of protection, as provided in the EU/EEA, was afforded in the third country of destination. This would allow a decision to be taken as to whether the transfers could continue. EUIs were then asked to report to EDPS any derogations used, any transfers that would continue to a third country that did not have an essentially equivalent level of protection, and any transfers that were suspended / terminated because of the absence of an essentially equivalent level of protection. EDPS would also explore the possibility of joint assessments of the level of protection of personal data afforded in third countries, and how these could be coordinated	

			between authorities, controllers and other stakeholders.	
32.	**European Data Protection Board**	**Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**	- These recommendations are an update of the previous analysis of the WP29, to identify the European Essential Guarantees, which need to be respected to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society. - These European Essential Guarantees are based on the jurisprudence of the Court of Justice of the European Union related to Articles 7, 8, 47 and 52 of the Charter of Fundamental Rights of the EU and, as the case may be, on the jurisprudence of the European Court of Human Rights related to Article 8 of the European Convention on Human Rights dealing with surveillance issues in States party to the ECHR. - the EDPB considers that the applicable legal requirements to make the limitations to the data	Recommendations 02/2020 on the European Essential Guarantees for surveillance measures | European Data Protection Board (europa.eu)

			protection and privacy rights recognised by the Charter justifiable can be summarised in four European Essential Guarantees: A. Processing should be based on clear, precise and accessible rules B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated C. An independent oversight mechanism should exist D. Effective remedies need to be available to the individual. - The Guarantees are based on the fundamental rights to privacy and data protection that apply to everyone, irrespective of their nationality. - The aim of the updated European Essential Guarantees is to provide a list of elements to examine whether, when transferring personal data, surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement	

			authorities, can be regarded as a justifiable interference or not. - The Essential Guarantees should not be assessed independently, as they are closely interlinked, but on an overall basis, reviewing the relevant legislation in relation to surveillance measures, the minimum level of safeguards for the protection of the rights of the data subjects and the remedies provided under the national law of the third country. The assessment of the third country surveillance measures against the Essential Guarantees may lead to two conclusions: • The third country legislation at issue does not ensure the EEG requirements: in this case, the third country legislation would not offer a level of protection essentially equivalent to that guaranteed within the EU. • The third country legislation at issue satisfies the EEG.	

33.	**European Data Protection Board**	**Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**	These recommendations follow from the Schrems II case in order to provide clarifications to the exporters within the scope of the GDPR on how to apply the GDPR and the ruling through the following 6 concrete steps: 1. The mapping of the (intended) transfers; 2. The verification of the transfer tool (intended to be) used; 3. The assessment of the legislation of the third country, including concerning the aspects related to access requests for national security purposes; ➔ Examining the legislation and the practices of the third country's public authorities to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred. Examining these practices will be especially relevant for the assessment where: (i) legislation in the third country formally meeting EU standards is manifestly not	Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

			applied/complied with in practice; or (ii) there are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking; or (iii) the transferred data and/or importer fall or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality). ➔ In the first two situations, suspension of the transfer or implementation of adequate supplementary measures to proceed with it. ➔ In the third situation, in light of uncertainties surrounding the potential application of problematic legislation to the transfer: either suspension of the transfer; implement supplementary measures to proceed	

			with it; or alternatively, proceed with the transfer without implementing supplementary measures if the exporter considers and is able to demonstrate and document that he/she has no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover the transferred data and importer. 4. The identification and adoption of supplementary measures; 5. The formal procedural steps to put in place; 6. The re-evaluation at appropriate intervals. - 3 Annexes also provide: definitions of the terms used, concrete scenario and examples of supplementary measures (technical, contractual, organisational), possible sources of information to assess	

			the third country's legal framework applicable to the transfers and practices. The assessment includes the legislation and practices of the third country of the importer in the field of access requests during the transfer, to data in transit from the EU to this country.	
34.	**European Data Protection Board**	**Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR**	**Content summary/main points:** - These guidelines are the first document providing, at EU level, a common understanding of the notion "transfer of personal data to third countries or international organisations" with a definition based on 3 cumulative criteria - The guidelines contain several examples of situations where, applying the criteria, data flows qualify or not as a transfer - The guidelines explain the consequences for organisations in case there is a transfer (to comply with the obligations of Chapter V of the GDPR and frame the transfer by using the instruments provided by the GDPR) and in case	Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR | European Data Protection Board (europa.eu)

			the transmission of data does not amount to a transfer (to implement measures if there is a risk for the data due to national laws in the third country of the importer) **Recommendations:** - Provide for a clear definition based on objective criteria of what is a transfer, what kind of entities can be involved in a transfer and what kind of operations can constitute a transfer - Provide for concrete examples and scenario/use case, in particular where the criteria to qualify a transfer are not met (for example the case of an employee traveling abroad accessing data of his company's data base) - Explain the obligations (contractual, technical, organisational) of the entities involved in a transfer - Even if the data flow does not qualify as a transfer, assess if there is a need to put in place specific additional safeguards in case of risks for the level of protection of the data because of the	

			local legislation or practices in the third country of the importer	
35.	**Ibero-American Network on Data Protection**	**Acuerdo Modelo De Transferencia Internacional De Datos Personales (Model Agreement For International Transfers Of Persona Data)**	The RIPD commissioned the elaboration of standard contractual clauses to facilitate the transfer of personal data from a data controller or processor established within the iberoamerican countries, to a controller or processor established in a third country that does not offer an adequate level of protection. As other documents, the RIPD model agreement offer model clauses applicable to transfers from controller to controller and from controller to processor. The document include in its different sections, definitions, limits to the modification of the clauses, applicable law, third part beneficiaries, duties of the parties, personal data principles, types of data, rights of the data subject, redress, and the role of the supervisory authority, amongst other issues. They set up a minimum	red-iberoamericana-clausulas-contractuales-2021.pdf (redipd.org)

			standard of data protection requirements for cross-border transfers to third countries. The Implementation Guidelines on Contractual Clauses must also be considered.	
36.	**Ibero-American Network on Data Protection**	**Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales (Guidelines for the Implementation of standard contractual clauses on international transfers of personal data)**	The RIPD, along the model agreement on international transfers, commissioned a document containing guidelines for the implementation of standard contractual clauses by the iberoamerican countries. This document includes a brief study of international transfers, most used mechanisms to ensure secure data transfers, the advantages and benefits of using standard contractual clauses, and practical issues regarding the implementation of such clauses.	red-iberoamericana-guia-implementacion-scc-2021.pdf (redipd.org)
37.	**Council of Europe Consultative Committee of the Convention for the Protection of Individuals**	**Draft paper: Draft Update of Council of Europe's contractual clauses in the context of transborder data flows (Prof. Pablo A Palazzi)**	• The draft paper sets out reasons why the current Council of Europe contractual clauses need to be updated: ○ International developments since the development of the clauses in 1992 and the Guide in 2002, including the	1680a48a73 (coe.int) NB: this is a not-for-citation draft, included only to highlight progress in updating the Council of Europe's SCCs)

	with regard to Automatic Processing of Personal Data		Additional Protocol regarding supervisory authorities and transborder data flows. ○ Many other international transfer regimes have developed or updated SCCs, including the EU; Ibero-American network; UK; New Zealand; ASEAN network. • The draft paper sets out the advantages of updated Council of Europe SCCs: providing companies with a ready-made and up to date 'tool' for transfers that takes into account C108+ requirements; contributing to convergence and bridging between different regions of the world (CoE covers three continents); providing predictability, legal certainty and building trust, while facilitating the free flow of data and protecting data subjects. • The draft paper sets out possible changes to make when updating the clauses, in the light of the principles of Convention 108+.	

38.	**Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**	**Draft Standard Contractual Clauses for Transborder Flows**	• This is a draft of the updated Council of Europe Standard Contractual Clauses for Transborder Flows. • Updates are made in the light of the principles of Convention 108+.	1680a5e7f5 (coe.int) NB: this is a not-for-citation draft, included only to highlight progress in updating the Council of Europe's SCCs)

Annex C: Data protection terms and their meanings: principles – analysis and report

GPA Global Frameworks and Standards Working Group

Data protection terms and their meanings: principles

1. Introduction

In 2020-21, the Global Frameworks and Standards Working Group (GFSWG, formerly known as Policy Strategy Working Group 1) analysed the core data protection terms defined in ten global data protection frameworks and developed a list of core terms and their high-level meanings that could be agreed across the GPA member authorities adhering to those frameworks. The analysis and list of terms and their meanings can be found in Annex F of the Policy Strategy WG 1: Global Frameworks and Standards annual report[6], adopted in October 2021.

On adoption of the report, it was agreed that the work on data protection terms would continue in 2021-22, and that it would focus on the meaning of core data protection principles.

Although mentioned in the report on last year's work on terms, it is worth repeating that terms and their meanings are vitally important. The work of the GFSWG since its establishment in 2019 has focused on identifying commonality in several aspects of global and regional privacy and data protection frameworks and instruments. In today's global digital environment, commonality and convergence have been highlighted as important elements in ensuring that data can flow across borders while retaining high levels of protection for the individuals it relates to.

Extending this project to attempt to define principles is challenging. Principles are not 'defined' in framework and instrument texts in the same way that the list of core data protection terms defined in our 2021 work often are. The approach to this stage of the work will therefore have a slightly different focus – rather than looking to 'define' the principles we are in reality looking to identify meanings by reference to the core elements of each principle, which will in turn allow us to identify commonality or otherwise.

2. Identifying the principles to define

In order to identify the principles to define, as a starting point the ten global frameworks analysed in our previous work were analysed again, to identify the most commonly found principles. The ten frameworks are as follows:

- Madrid Resolution
- OECD Privacy Guidelines
- APEC Privacy Framework
- Council of Europe Convention 108
- Council of Europe Convention 108+
- Standards for Personal Data Protection for Ibero-American States

[6] 1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org)

- African Union Convention on Cyber Security and Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files
- ECOWAS Supplementary Act on Personal Data Protection

The most commonly-found principles in the ten global frameworks, and the relevant extracts from each text, can be found in Annex 1 below. The principles are:

- Fairness (found in all ten frameworks)
- Lawfulness (found in all ten frameworks)
- Purpose specification (found in all ten frameworks)
- Proportionality (found in all ten frameworks)
- Data quality (found in all ten frameworks)
- Transparency (found in eight frameworks)
- Accountability (found in six frameworks)
- Security (found in all ten frameworks)
- Data retention (found in eight frameworks)

There were a few instances of other aspects of privacy and data protection being included as principles in some frameworks, for example data subject rights, and conditions for the processing of sensitive/special categories of data. However, these were not so commonly found as principles in the frameworks, so have not been included in the list.

Additionally, as some of the ten frameworks analysed are now several years old, we considered a small selection of other texts - a recently-updated regional framework (the Organisation of American States' 2021 Updated Principles on Privacy and Personal Data Protection[7]) and two recently developed/amended laws (Japan's 2020 amended Act on the Protection of Personal Information[8], and Brazil's General Data Protection Law[9]) to check whether principles in the newer texts were generally consistent with the ten frameworks. We found general consistency across the ten global frameworks and the three other instruments, as follows:

The OAS Updated Principles on Privacy and Personal Data Protection includes principles relating to: Lawful purposes and loyalty (covering lawfulness and fairness); Transparency and consent; Relevance and necessity (covering proportionality); Limited processing and retention (covering purpose specification and data retention); Confidentiality; Security; Accuracy (data quality); and Accountability. The OAS Principles also included data subject rights, conditions for sensitive personal data, cooperation on trans-border data flows, conditions for exceptions, and the

[7] Publication Updated Principles on Privacy and Protection of Personal Data 2021.pdf (oas.org)
[8] Amended Act on the Protection of Personal Information(June 2020) (Tentative Translation) -Personal Information Protection Commission, Japan- (ppc.go.jp) – unofficial translation
[9] Brazilian General Data Protection Law (LGPD, English translation) (iapp.org) – unofficial translation

establishment of independent authorities as principles – but as these are not so commonly-found as principles in other instruments they will not be included in our list of principles to analyse.

Japan's amended Act on the Protection of Personal Information includes principles relating to: purpose specification; fairness and lawfulness (to an extent); transparency; data quality; data retention; and security. Of the commonly found principles in other global frameworks, the Japanese law does not appear to directly refer to accountability or proportionality principles in terms, although other principles and obligations in the Act seem to create similar effects. Additional principles included in the Act include conditions relating to sensitive/special categories of data.

In Brazil's General Data Protection Law (LGPD) the commonly-found principles are generally included, with similar core elements to those in the global frameworks analysed. Some minor differences exist: there are no specific principles relating to fairness and lawfulness, however the non-discrimination principle refers to the "impossibility of carrying out the processing for unlawful or abusive discriminatory purposes", therefore including unlawfulness and implying an element of fairness. In addition, data retention is not included as a principle, however a later article makes provision that processing should be terminated "when no longer necessary or pertinent to achieve the specific purpose intended" – again including similar core elements to those in the analysed frameworks.

We have therefore analysed the meaning of all nine data protection principles listed above.

3. Analysis of commonality and difference

The table in Annex 2 below lists the principles whose meaning was analysed as part of this project. The table also includes the analysis results, setting out the common elements in the descriptions of the principles in each of the frameworks.

In the main there can be seen quite substantial commonality in the way the principles are described.

In particular the descriptions of lawfulness, purpose specification, data quality, security and data retention can be seen to have strong commonalities:

- **Lawfulness** is described in most of the frameworks by reference to respecting or adhering to the law, although some frameworks add a requirement to have a specific basis in law for the processing (some go on to provide a list of specific bases for processing).
- **Purpose specification** is clearly described in three frameworks by reference to processing being limited to specific, explicit and legitimate purposes, while most of the frameworks use reference to compatibility – that processing must be compatible (or not incompatible) with the original purposes for processing.
- **Data quality** is described in most frameworks in relation to personal data being accurate, complete and up to date. A smaller number of frameworks go on to set out that personal data that is inaccurate or incomplete should be erased or rectified.

- **Security** is described by reference to protecting personal data with appropriate measures against varying combinations of unauthorised or accidental loss, destruction, access, use, modification or disclosure. One framework adds protection against unlawful processing, while another two frameworks set out that the aim of the principle is to ensure integrity, confidentiality and availability of the data.
- **Data retention** is described using minor variations of the themes of personal data being retained in a form that permits identification for no longer than necessary for the purposes, and being deleted or rendered anonymous when no longer needed.

The remaining four principles – fairness, proportionality, transparency and accountability - are described in some areas with differing areas of focus so commonalities are not as strong. However there are no major inconsistencies between the descriptions:

- **Fairness** is described using slightly different approaches across the frameworks. Some focus on the avoidance of discrimination, whereas others are more concerned that personal data is obtained and processed non-fraudulently. Additionally, several frameworks focus on the importance of the data subject being informed about the processing of their personal data.
- **Proportionality** is approached in varying degrees, with three frameworks describing it as processing limited to the minimum necessary. Not all frameworks use reference to limitations in their descriptions, but almost all refer to processing that is adequate and relevant to the purpose. About half refer to “limited” or “not excessive”.
- **Transparency** is again approached in varying degrees - most of the frameworks imply that transparency involves the provision of information to data subjects, but one suggests that the information should be readily available, implying a less active approach. Some frameworks provide much more detailed requirements as to what constitutes transparency, setting out specific items of information that should be provided. One framework further specifies that information should be concise, accessible and easy to understand, that clear and plain language be used, particularly when addressed to a child.
- Finally, while the high level description of **accountability** is fairly consistent, focusing on the implementation of measures to comply with, or to be able to demonstrate compliance with, data protection and privacy obligations, there are minor differences in relation to who the controller / person responsible should be accountable to (supervisory authorities and/or data subjects), as well as in how accountability can be demonstrated, with some frameworks, for example, suggesting privacy management programmes.

While there are some differences in approach as described above, there can be seen substantial commonality between data protection and privacy principles across the frameworks. This would seem to support findings in earlier analyses that identified positive levels of commonality and convergence in data protection law and frameworks, and may be helpful to highlight in the increasingly globalised digital world as we continue to seek ways of protecting data both within and across borders.

4. Conclusion: the GPA's list of core privacy and data protection principles, and their meanings

The commonality identified, at least at a high level, indicates that it may be possible to set out high level meanings or descriptions of each principle that, while not being identical to descriptions in any one framework could be broadly consistent, or at least not contradictory. The principles and their high level meanings are set out in the table immediately below.

It is hoped that the commonality identified can act as a positive addition to the conversation on the importance of interoperability between frameworks.

Privacy and data protection principles, and their meanings

Principle	Meaning
Fairness	Respecting the rights and freedoms of individuals when processing personal data, by obtaining and further processing it non-fraudulently, transparently and in a way that does not give rise to discrimination.
Lawfulness	Processing personal data in a way that respects applicable laws, rights and freedoms. Where required, a basis in law must be identified for processing to be lawful.
Purpose specification	Processing of personal data is limited to specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes.
Proportionality	Processing of personal data is limited to that which is adequate, relevant and not excessive in relation to the purpose.
Data quality	Measures shall be taken to ensure that personal data shall be accurate, complete and kept up to date, to the extent necessary for the purposes.
Transparency / openness	Being open, and providing clear information, about all the aspects of the processing of personal data. **Sometimes referred to as openness; notice**
Accountability	Implementing measures or mechanisms which demonstrate compliance with privacy and data protection obligations.

Security	The protection of personal data with appropriate measures (which may be technical, organisational or physical) against risks such as accidental or unauthorised loss, access, damage, destruction, use, modification or disclosure.
Data retention	Personal data shall be retained in a form that permits identification for no longer than is necessary for the purposes for which the data is processed, after which it should be deleted or anonymised.

Annex 1: Data protection principles in the 10 frameworks analysed in 2019-20 by GPA Policy Strategy Working Group 1: Global frameworks and standards, and their descriptions

Note: There are no formal definitions of data protection principles in the frameworks. Instead, following on from the approach taken in 2020-21, in the absence of formal definitions we have extracted the meanings indirectly set out in the frameworks, usually by reference to the essential elements of the principle.

	Madrid Resolution	**OECD Privacy Guidelines**	**APEC Privacy Framework**	**Convention 108**	**Convention 108+**	**Standards for Personal Data Protection for Ibero-American States**	**African Union Convention on Cyber Security and Personal Data Protection**	**EU General Data Protection Regulation**	**UN Guidelines for the Regulation of Computerized Personal Data Files**	**ECOWAS Supplementary Act on Personal Data Protection**
Principles										
Fairness	**Principle of lawfulness and fairness** – Personal data must be fairly processed, respecting the	**No standalone principle – included in the Collection limitation principle –** There should be limits to the	**No standalone principle – included in the Collection limitation principle** – Information should be obtained by	**No standalone principle – included in the Quality of data principle –** Personal data shall be obtained and	**No standalone principle – included in the Legitimacy of data processing and quality of data principle –**	**Loyalty principle –** The person responsible shall treat personal data - protecting the holders' best interest. -	**Principle of lawfulness and fairness of personal data processing –** The collection, recording,	**Lawfulness, fairness and transparency principle –** Personal data shall be processed lawfully,	**Principle of lawfulness and fairness –** Information about persons should not be collected or processed in unfair or	**Principle of legality and fairness –** The collection, recording, processing, storage, and transmission of personal data must be

	applicable national legislation as well as the rights and freedoms of individuals as set out in the Resolution and in conformity with the purposes and principles of the Universal Declaration of Human Rights and the	collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. The section on National Implementation sets out that in implementing the Guidelines, "Member	lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. Examples are given in the commentary: "So, for example, obtaining personal information under false pretenses (e.g., where an organization uses	processed fairly and lawfully. **Recommendation CM/Rec (2010)13 and explanatory memorandum: on The protection of individuals with regard to automatic processing or personal data in the context of profiling –**	Data processing shall (…) reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. Personal data undergoing processing shall be processed	refraining from treating the data through deceiving or fraudulent means. Treatment that results in unfair or arbitrary discrimination against holders shall be considered unfair.	processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently.	fairly and in a transparent manner in relation to the data subject. **Recital 42** – Where processing is based on the data subject's consent […] a declaration of consent […] should not contain unfair terms.	unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.	carried out in a legal, fair and non-fraudulent manner.

	International Covenant on Civil and Political Rights. Processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.	countries should […] ensure that there is no unfair discrimination against data subjects."	phishing, telemarketing calls, or pretexting emails to fraudulently misrepresent itself as another company in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal	In the Explanatory Memorandum's Comments on the provisions of the recommendation it is noted that "profiling is often used without the knowledge of the individuals concerned and may therefore undermine the fairness of data processing in so far as	fairly and in a transparent manner. Additionally in **Article 8 – Transparency of processing-** It is noted that "Each Party shall provide that the controller informs the data subjects of […] as well as any necessary additional			**Recital 60** – The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. **Recital 71** – In order to ensure fair and transparent processing		

			information) may in many economies be considered unlawful. Therefore, even in those economies where there is no explicit law against these specific methods of collection, they may be considered to be unfair	the data subjects are unaware of the existence or logic of their profiling."	information in order to ensure fair and transparent processing of the personal data."			[…] prevent discriminatory effects.		

			means of collection."							
Lawfulness	**Principle of lawfulness and fairness** – Personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedoms as set out in the Resolution in	**No standalone principle – included in the Collection limitation principle –** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate	**No standalone principle – included in the Collection limitation principle** – information should be obtained by lawful and fair means, and where appropriate , with notice to, or consent of, the individual concerned.	**No standalone principle – included in the Quality of data principle –** Personal data shall be obtained and processed fairly and lawfully.	**Legitimacy of data processing and quality of data principle –** Personal data undergoing processing shall be processed lawfully. Article 5.2 Each Party shall provide that data processing can be carried out on the basis	**Lawfulness principle –** Strict adherence to internal State law, international law, individual rights and freedoms. Public authorities' treatment of personal data is subject to powers granted to them by law.	**Principle of lawfulness and fairness of personal data processing –** The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-	**Lawfulness, fairness and transparency principle –** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject . **Article 6** sets out specific bases for	**Principle of lawfulness and fairness –** Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the	**Principle of legality and fairness –** The collection, recording, processing, storage, and transmission of personal data must be carried out in a legal, fair and non-fraudulent manner. **Principle of consent and legitimacy –** Processing is legitimate

	conformity with the purposes and principles of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.	, with the knowledge or consent of the data subject.			of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.	**Legitimation principle –** Person responsible can only treat personal data if: - holder consents - necessary for compliance with court order, resolution, competent public authority mandate - necessary for exercise	fraudulently. **Principle of consent and legitimacy of personal data processing –** Processing will be deemed legitimate where the data subject has given his/her consent, or where the processing is necessary for:	processing, one of which must apply if processing is to be lawful. Lawful bases include consent of the data subject, necessary for performance of a contract to which the data subject is party, necessary for legal obligation to which	United Nations.	where the data subject has given consent. Consent requirement can be waived when the processing is necessary: - to comply with a legal obligation - for implementation of a public interest mission or relevant to the exercise of public authority vested in the controller

						of public authority powers - necessary for defence of holder's rights before a public authority - necessary for agreement/ pre - agreement - necessary for compliance with a legal obligation - necessary for vital interests	- controller's compliance with a legal obligation - performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or a third party - performance of a	the controller is subject, necessary to protect vital interests, necessary for tasks carried out in the public interest or in the exercise of official authority, necessary for the purposes of legitimate interests.		- for performance of a contract to which the data subject is party or for the application of pre – contractual measures at their request - for safeguarding the interests or rights and fundamental liberties of the data subject.

						- necessary for public interest reasons established or provided by law - necessary for the legitimate interests of the person responsible or third party.	contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract - protect the vital interests or fundamental rights and freedoms of the data subject.			
Purpose specification	**Purpose specificati**	**Purpose specificatio**	**Uses of personal**	**No standalone principle –**	**No standalone principle –**	**Purpose principle –**	**Principle of purpose, relevance,**	**Purpose limitation principle –**	**Principle of the purpose**	**Principle of purpose, relevance**

	on principle – Personal data should be limited to the fulfilment of the specific, explicit and legitimate purposes of the responsible person; no processing that is non-compatible with the purposes for which	**n principle** – specified … and limited to the fulfilment of those purposes ... or such others as are not incompatible with those purposes.	**information principle** – used only to fulfil the purposes of collection and other compatible or related purposes except with consent, where necessary to provide a requested service or product, by the authority of law.	**included in the Quality of data principle –** Personal data (…) shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.	**included in the Legitimacy of data processing and quality of data principle –** Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with	defined, explicit and legitimate purposes.	**and storage of processed personal data –** Data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes.	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	**specification –** The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to	**and preservation –** Personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes.

	personal data was collected, unless unambiguous consent of the data subject is given.				those purposes.				make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the	

									person concerned, for purposes incompatible with those specified; (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.	
Proportionality	**Proportionality principle** –	**No standalone principle – included in**	**No standalone principle – included in**	**No standalone principle – included in**	**No standalone principle – included in**	**Proportionality principle –**	**Principle of purpose, relevance, and storage**	**Data minimisation principle –**	**Principle of the purpose specification –**	**Principle of purpose, relevance and**

	Personal data processing should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes so specified. Processed personal data limited to the minimum necessary.	**the Collection limitation principle and the Data quality principle –** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate , with the knowledge or consent	**the Collection limitation principle** – Collection should be limited to information relevant to the purposes.	**the Quality of data principle –** Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.	**the Legitimacy of data processing and quality of data principle –** Data processing shall be proportiona te in relation to the legitimate purposes pursued and reflect at all stages a fair balance between all interests concerned , whether	The person responsible shall only treat personal data that is appropriate , pertinent and limited to the minimum necessary for the purpose.	**of processed personal data –** Data collection shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible	**preservation –** Personal data [...] shall be adequate and relevant in relation to the purposes for which it is collected and further processed.

		of the data subject. Personal data should be relevant to the purposes for which they are to be used.			public or private, and the rights and freedoms at stake. Personal data under - going processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.				subsequentl y to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified.	
Data quality	**Data quality principle** –	**Data quality principle –**	**Integrity of personal**	**Quality of data principle** –	**Legitimacy of data processing and quality**	**Quality principle –**	**Principle of accuracy of**	**Accuracy principle –**	**Principle of accuracy –**	**Principle of accuracy –**

	The responsible person should at all times ensure that personal data are accurate, sufficient and kept up-to-date to fulfil the purposes for which they are processed. Retention period of processed personal data limited to	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	**information principle** – Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes.	Personal data (…) shall be accurate and, where necessary, kept up to date and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.	**of data principle –** Personal data undergoing processing shall be accurate and, where necessary, kept up to date and preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which	The person responsible shall adopt necessary measures to keep personal data accurate, complete and updated.	**personal data –** Data collected shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were	Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified	Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to	Personal data obtained shall be accurate and, where necessary, kept up to date. All reasonable measures shall be undertaken to ensure that data that is inaccurate and incomplete in relation to the purposes for which it is obtained and further processed shall be erased or rectified.

	the minimum necessary, when personal data are no longer necessary to fulfil the purposes which legitimized their processing they must be deleted or rendered anonymous.				those data are processed.		collected/ further processed, are erased or rectified.	without delay.	avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.	
Openness / transparency	**Openness principle** –	**Openness principle** –	**Notice principle** –		**Transparency of**	**Transparency principle –**	**Principle of transparency of personal**	**Lawfulness, fairness and transparenc**		**Principle of transparency –**

	Every responsible person shall have transparent policies with regard to the processing of personal data. 2. The responsible person shall provide to the data subjects, as a minimum, information about	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main	Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected;		**processing principle –** 1. Each Party shall provide that the controller informs the data subjects of: a. his or her identity and habitual residence or establishment; b. the legal basis and the purposes of the	16.1. The person responsible shall inform holder about the existence and main characteristics of the treatment to which its personal data shall be submitted, in order to make informed decisions on this regard. 16.2. The person responsible	**data processing –** Requires mandatory disclosure of information on personal data by the controller.	**y principle –** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. **Also in Recital 39 –** Any processing of personal data should be […] transparent to natural persons		The principle of transparency implies that the data controller is obliged to provide information about the processing of personal data.

	the responsible person's identity, the intended purpose of processing, the recipients to whom their personal data will be disclosed and how data subjects may exercise the rights provided in this Document	purposes of their use, as well as the identity and usual residence of the data controller.	b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information		intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal data, if any; and e. the means of exercising the rights set out in Article 9,	shall provide holder, at least the following information: a. Its identity and contact information. b. The purposes of the treatment to which its personal data shall be submitted. c. The communications,		that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communica		

	, as well as any further information necessary to guarantee fair processing of such personal data. 3. When personal data have been collected directly from the data subject, the information must be		on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting,		as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.	whether national or international, of personal data that it intends to perform, including the recipients and the purposes that give rise to the performance thereof. d. The existence, form and mechanisms or procedures through which it		tion relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the		

	provided at the time of collection, unless it has already been provided. 4. When personal data have not been collected directly from the data subject, the responsible person must also inform him/her about the		their personal information. This Principle is directed towards ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information			may exercise the access, correction, cancellation, opposition and portability rights. e. If applicable, the origin of the personal data when the person responsible did not obtain them directly from holder.		purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which		

	source of personal data. This information must be given within a reasonable period of time, but may be replaced by alternative measures if compliance is impossible or would involve a disproportionate effort by the		controllers may enable an individual to make a more informed decision about interacting with the organization.			16.3. The information provided to holder must be sufficient and easily accessible, as well as written and structured in a clear and simple language, easy for holders to whom it is addressed to understand, especially in the case of girls, boys and		are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes		

	responsible person. 5. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed					adolescents. 16.4. Every person responsible shall have transparent policies for the treatment of the personal data that it performs.		for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. **Also in Recital 58 –** The principle of transparency requires that any information addressed		

	specifically to minors. 6. Where personal data are collected on line by means of electronic communications networks, the obligations set out in the first and second paragraphs of this section may be satisfied by posting privacy							to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic		

	policies that are easy to access and identify and include all the information mentioned above.							form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and		

								understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where		

								processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.		
Accountability	**Accountability principle** – The responsible person shall take all necessary measures to observe the	**Accountability principle** – A data controller should be account - able for complying with measures which give	**Accountability principle** – controller should be accountable for complying with measures that give effect to		**No standalone principle – included in Article 10: Additional obligations** – each Party shall provide that Controllers	**Responsibility principle** – The person responsible shall implement necessary mechanisms to prove compliance, shall be		**Accountability principle** – The controller shall be responsible for, and be able to demonstrate compliance		

	principles and obligations set out in this Resolution and in the applicable national legislation and have the necessary internal mechanism in place for demonstrating such observance both to data subjects and to the supervisor	effect to the principles stated above. A data controller should: a) Have in place a privacy management programme and be prepared to demonstrate the programme as appropriate, in particular at the request	the principles. When information is transferred to another, the controller should obtain consent or exercise due diligence, taking reasonable steps to ensure that the recipient will protect the information in line with		and, where applicable, processors , take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate that the data processing under their control is in compliance.	accountable to the holder and to the control authority. Mechanisms to adopt may be: - data protection programs and policies - risk management systems - training - reviews of policies and programs - audits		with, paragraph 1 [the principles] **Also in Article 24: Responsibility of the controller –** The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that		

	y authorities in the exercise of their powers as established under section on Compliance and monitoring: Independent Supervisory authorities powers and competences.	of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines.	the principles.			- complaints procedures.		processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.		

Security	**No standalone principle – included in Part V: Security** – Both the responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical and organizati	**Security safeguards principle –** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	**Security Safeguards principle –** appropriate safeguards against loss/ unauthorised access; unauthorised destruction, use, modification, disclosure.	**Data security principle –** Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against	**Data security principle –** Each party shall provide that the controller, and where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modificatio	**Safety principle –** The person responsible shall establish and maintain sufficient administrative, physical and technical measures in order to guarantee the confidentiality, integrity and availability of personal data.	**Principle of confidentiality and security of personal data processing –** Personal data shall be processed confidentially and protected, in particular where the processing involved transmission of the data over a network. Controllers and	**Integrity and confidentiality principle –** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against	**Principle of security –** Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by	**Principle of confidentiality and security –** Personal data shall be processed confidentially and shall be protected, in particular when processing includes transmission of data on a network. **Also Article 43: Obligations of security –** The data controller shall take all

	onal measures to ensure, at each time, their integrity, confidentiality and availability.			unauthorised access, alteration or dissemination.	n or disclosure of personal data.		processors must ensure compliance with security measures defined in this Convention. **Article 21: Security obligations –** the data controller must take all appropriate precautions, according to the nature of the data,	accidental loss, destruction or damage, using appropriate technical or organisational measures. **Also in Article 32: Security of processing –** Taking into account the state of the art, the costs of implementation and the nature, scope,	computer viruses.	necessary precautions in relation to the nature of data, and in particular to ensure that it is not deformed, damaged or accessible to unauthorised third parties.

							and in particular, to prevent such data from being altered or destroyed, or accessed by unauthorized third parties.	context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures		

								to ensure a level of security appropriate to the risk.		
Data retention	**No standalone principle – included in the Data quality principle:** The responsible person shall limit the period of retention of the processed personal data to			**No standalone principle – included in the Quality of data principle –** Personal data shall be preserved in a form which permits identification of the data subjects for no longer	**No standalone principle – included in the Legitimacy of data processing and quality of data principle –** Personal data undergoing processing shall be preserved in a form which	**No standalone principle – included in the Quality principle –** When personal data is no longer necessary for the purpose, the person responsible shall delete or remove it from its archives,	**Principle of purpose, relevance, and storage of processed personal data –** Data shall be kept for no longer than is necessary for the purposes for which the data were collected or	**Storage limitation principle –** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal	**Principle of the purpose specification –** The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain	**Principle of purpose, relevance and preservation –** Personal data […] shall be kept for a period which shall not exceed the period required for the purposes for which they were obtained and processed.

	the minimum necessary. When personal data are no longer necessary to fulfil the purposes they must be deleted or rendered anonymous.			than is required for the purpose for which those data are stored.	permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed .	records, databases, files, systems, or anonymize it.	further processed. Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law. **Article 22:** Storage obligations – personal data shall	data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article	amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the	Beyond the required period, data may only be kept with a view to responding specifically to processing for historical, statistical and research purposes, in line with existing legal provisions. **Also Article 44: Obligations of preservation –** Personal data shall be kept for a period of

							be kept no longer than is necessary for the purposes for which the data were collected or processed.	89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.	purpose so specified.	time set by a regulatory text and only for the purposes for which they were obtained.

Annex 2 – Data protection principles and their meanings: commonalities across the frameworks

Principle	Frameworks including the principle	Comments: Common elements	Comments: Any significant differences between frameworks	Dictionary definition, where relevant
Fairness	All 10	- respecting / reflecting the rights and freedoms of individuals (2) - obtaining data by fair means (3) - not giving rise to unlawful or arbitrary discrimination (2) - no unfair discrimination - prevent discriminatory effects - information not obtained under false pretences / fraudulent means (2) - processing should be undertaken non-fraudulently (2)	No significant difference. Frameworks do tend to take slightly different approaches – some focus on the avoidance of discrimination, whereas others are more concerned that personal data is obtained and processed non-fraudulently. Several frameworks focus on the importance of the data subject being informed about the processing of their personal data.	'Fair' - Impartial, just, equitable, reasonable

		- processing without the knowledge of individuals is unfair - subject should be informed of the processing and its purposes - reflecting a balance between all interests concerned		
Lawfulness	All 10	- respecting applicable national legislation - processing should be carried out on a legitimate basis laid down by law - strict adherence to internal State law, international law, individual rights and freedoms - public authority processing subject to powers granted to them by law	No significant difference. Several frameworks go on to specify bases for processing that must apply for the processing to be lawful.	'Lawful' - Allowed by law

		- must have a specific basis for processing (5) - processing carried out in a legal manner		
Purpose specification	All 10	- processing limited to the fulfilment of specific, explicit and legitimate purposes (3) - no processing that is not compatible with the purposes for which the personal data was collected - used only to fulfil the purposes of collection and other compatible or related purposes - not further processed in a way incompatible with the original purposes (5)	No significant difference.	
Proportionality	All 10	- processing limited to the minimum necessary (3) - processing limited to that which is adequate (7), relevant (9) / appropriate/pertinent (1)	No significant difference. Some differences of degree exist – two frameworks refer to	

		and not excessive (4) in relation to the purpose	only 'adequate and relevant', with no specific reference to limitations. The remaining frameworks refer to either 'limited' (5), or 'not excessive' (4), or both.	
Data quality	All 10	Measures shall be taken to ensure that personal data shall be accurate (10), sufficient (1) / complete (6), and kept up to date (10), to the extent necessary for the purposes (8) Personal data that is inaccurate (3) or incomplete (2) in relation to the purposes should be erased or rectified.	No significant difference.	
Transparency / openness	8 – all bar C108; UN Guidelines	Informing / providing information / openness about the processing of personal data.	No significant difference. Most of the frameworks imply that transparency involves the provision of information to data	Openness.

			subjects, but one suggests that the information should be readily available. Some frameworks provide much more detailed requirements as to what constitutes transparency, setting out specific items of information that should be provided. One framework further specifies that information should be concise, accessible and easy to understand, that clear and plain language be used, particularly when addressed to a child.	
Accountability	6 – Madrid Resolution; OECD; APEC Privacy Framework; C108+;	Implementing measures / mechanisms to comply with (5) being able to demonstrate compliance with (3) the principles/obligati ons.	No significant difference. Some frameworks specify who controllers should be accountable to – to supervisory	The fact or condition of being accountable; responsibility; being able to

	Ibero-American Standards; GDPR		authorities (3) and data subjects (2). Others do not. Some frameworks give examples of how accountability can be ensured / demonstrated, such as the use of privacy management programmes. Others do not.	give a satisfactory reason for actions.
Security	All 10	Protecting personal data - with appropriate (7) reasonable (1) technical (3) organisational (2) administrative (1) physical (1) / security (3) / measures (7) safeguards (2) precautions (2) - to ensure integrity, confidentiality and availability (2) - against such risks as loss or unauthorised access,	No significant difference.	The state or means of being secure, protection.

		destruction, use, modification or disclosure (2) - against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination - against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure - prevent data from being altered or destroyed, or accessed by unauthorized third parties - against unauthorised or unlawful processing and against accidental loss, destruction or damage		
Data retention	8 – all bar OECD Privacy Guidelines	- retention period limited to the minimum necessary / shall not	No significant difference.	

	and APEC Privacy Framework.	exceed the period required for the purposes (2) - personal data are deleted or rendered anonymous when they are no longer necessary to fulfil the purposes (2) - preserved in a form that permits identification no longer than is necessary for the purposes (3)	Three frameworks specify that personal data may be stored for longer periods solely for historical, statistical or research purposes.	

GPA glossary of data protection terms and their meanings

October 2022

GPA glossary of data protection terms and their meanings

The GPA Global Frameworks and Standards Working Group completed an analysis of privacy and data protection terms and their meanings in 2021 and 2022. Ten global data protection frameworks were analysed in relation to how they defined or described core data protection terms. This glossary lists the terms analysed and their meanings as adopted by the GPA in 2021[10] and 2022[11].

It should be noted that the meanings are not intended to be legal definitions, nor are they intended to represent exact definitions found in all global data protection frameworks and instruments. Instead, they provide practical shared meanings common to most frameworks across the globe.

Data

Term	Meaning
Personal data	Any information relating to an identified or identifiable individual. Examples could include name, address and other personal details; account numbers; IP addresses; medical, banking, education or employment details, as well as many others. Sometimes referred to as **personal information**.
Sensitive data	Personal data that affects the most intimate sphere of the data subject, or may give rise to discrimination or serious risk. This can include data that reveals or relates to racial or ethnic origin; political opinions; trade union affiliation; religious or philosophical beliefs; health; sex life or orientation; criminal proceedings or convictions; or biometric and genetic data. Sometimes referred to as **sensitive categories of data; sensitive personal data; special categories of personal data**.

Actors in the processing of personal data

Term	Meaning

[10] Adopted with the GPA Policy Strategy Working Group: Global Frameworks and Standards annual report in October 2021.

[11] TBC – will be submitted for adoption at the October 2022 GPA Closed Session.

Data subject	An identified or identifiable individual to whom the personal data relates directly or indirectly. Referred to as the **holder** in the Ibero-American Standards.
Controller	Any natural or legal person, public or private body who, alone or jointly with others, decides the purpose and the means of processing the personal data. Sometimes referred to as the **data controller; personal information controller; controller of the file; responsible person; person responsible**.
Processor	Any natural or legal person, public or private body that processes personal data on behalf of the controller. Sometimes referred to as the **data processor; personal information processor; processing service provider; person in charge; sub-contractor**.
Third party	Any natural or legal person, or public authority or body other than the data subject, controller, processor or person who is under the direct authority of the controller or processor and authorised to process the personal data.

Actions in the processing of personal data

Term	Meaning
Processing	Any operation or set of operations performed on personal data. This can include collection; recording; extraction; organisation; structuring; storage; use; disclosure; making available; accessing; erasure; destruction; alteration; and encryption. Sometimes referred to as **use; treatment.**
Profiling	Any form of automated processing that applies a profile to an individual, using their personal data to evaluate certain personal aspects relating to that person. In particular this may be to take

	decisions concerning the person, or to analyse or predict personal preferences, behaviours, attitudes and aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, location or movements.
Anonymisation	The application of measures aimed at making personal data anonymous so that a data subject is not, or is no longer, directly or indirectly identifiable.
Pseudonymisation	The processing of personal data in order that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information must be kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to and identified or identifiable natural person.
Personal data breach	A breach in the security of personal data, leading to accidental or unlawful: loss; modification; destruction; unauthorised disclosure of, or access to, personal data. Sometimes referred to as a **data breach; security breach**.

Key concepts

Term	Meaning
Consent	The agreement or acceptance of the data subject to the processing of their personal data, by way of the expression of freely given, specific, clear, unambiguous, informed indication of their wishes.
Accountability	Implementing measures or mechanisms which demonstrate compliance with privacy and data protection obligations.
Transparency	Being open, and providing clear information, about all the aspects of the processing of personal data. Sometimes referred to as **openness; notice**.

Measures

Term	Meaning
Privacy / data protection by design and default	Where technologies, processes and practices are built into system architectures, rather than being added as an afterthought, and processing is designed in such a manner to comply, from the outset, with data protection rules and minimise privacy and data protection risk.
Privacy / data protection impact assessment	An assessment of the impact of envisaged personal data processing on the risks to individuals' privacy rights.
Privacy management programme	An operational mechanism through which organisations implement privacy protection and demonstrate compliance.

Supervision and enforcement

Term	Meaning
Supervisory authority	An independent authority responsible for monitoring the application of data protection and privacy laws, including enforcement. Sometimes referred to as a **privacy enforcement authority; control/supervision authority; national personal data protection authority; authority of protection**.

Principles

Term	Meaning
Fairness	Respecting the rights and freedoms of individuals when processing personal data, by obtaining and further processing it non-fraudulently, transparently and in a way that does not give rise to discrimination.

Lawfulness	Processing personal data in a way that respects applicable laws, rights and freedoms. Where required, a basis in law must be identified for processing to be lawful.
Purpose specification	Processing of personal data is limited to specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes.
Proportionality	Processing of personal data is limited to that which is adequate, relevant and not excessive in relation to the purpose.
Data quality	Measures shall be taken to ensure that personal data shall be accurate, complete and kept up to date, to the extent necessary for the purposes.
Transparency / openness	Being open, and providing clear information, about all the aspects of the processing of personal data. **Sometimes referred to as openness; notice**
Accountability	Implementing measures or mechanisms which demonstrate compliance with privacy and data protection obligations.
Security	The protection of personal data with appropriate measures (which may be technical, organisational or physical) against risks such as accidental or unauthorised loss, access, damage, destruction, use, modification or disclosure.
Data retention	Personal data shall be retained in a form that permits identification for no longer than is necessary for the purposes for which the data is processed, after which it should be deleted or anonymised.