Policy Strategy Working Group 1: Global frameworks and standards

Report – July 2021

Chair authority: UK Information Commissioner's Office

Table of Contents

Executive Summary

Policy Strategy Working Group 1: Global frameworks and standards was established in 2019-20 after the adoption of the Resolution on the Conference's strategic direction[1] in Tirana in 2019. The resolution adopted the GPA's Strategic Plan for 2019-21, which included, for the first time, a Policy Strategy.

The Policy Strategy intended to implement the GPA's first strategic priority of working towards a global regulatory environment with clear and consistently high standards of data protection, and to strengthen the GPA's policy role in influencing and advancing privacy and data protection at an international level – all year round.

The first pillar of the Policy Strategy, Global frameworks and standards, encompassed the theme of evolution towards global policy and standards. Policy Strategy Working Group 1: Global frameworks and standards (PSWG1) was created to deliver two specific actions around this theme, namely:

1. To complete an analysis of current frameworks for privacy and data protection, including key principles, data subject rights, cross border transfers and demonstrable accountability standards.
2. To consider developing common definitions of key data protection terms.

PSWG1 delivered the frameworks analysis in 2019-20, and it was adopted as an annex to the PSWG1 annual report[2]. The analysis has proven to be a useful piece of work in its own right, with positive feedback received and several instances of external organisations and GPA members referring to it while working on related issues. Most recently, the analysis has been referenced in the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[3], where it is recommended as a resource for data controllers to assess a third country for suitability for data transfers from the EU.

In 2020-21, PSWG1 has worked on several specific topics to follow on from the 2020 frameworks analysis, and to deliver our second allocated Policy Strategy action; these are:

- Further analysis of cross border transfer mechanisms
- Key features of independent data protection authorities
- Government access to personal data
- Common definitions of data protection terms

[1] Global Privacy Assembly, Resolution on the Conference's Strategic Direction 2019-21, adopted October 2019
[2] Global Privacy Assembly, Policy Strategy Working Group 1: Global frameworks and standards Annual Report, adopted October 2020
[3] 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, Version 2.0, adopted 18 June 2021

PSWG1 submits the reports and other outputs from the above topics for adoption by the Closed Session as annexes to this annual report. In addition, at the time of writing, a draft resolution is being considered on the topic of government access to personal data and may be submitted for adoption at the Closed Session.

PSWG1 is pleased to note that the new draft GPA Strategic Plan 2021-23 recognises the importance of global frameworks and standards, and has allocated two broad actions to the WG. In 2021-23 PSWG1 will therefore carry out work on the following:

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

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

- continue with the next phase of work on data protection terms. In 2021-22 the focus will be on the meaning of terms relating to core data protection principles

- continue with work on cross border transfer mechanisms. As a starting point, this year's report and any recommendations will be considered.

PSWG1 may request the support and expertise of the new GPA Reference Panel to assist with certain aspects of the above topics.

Introduction

As mentioned in the previous section, PSWG1 was established in 2019-20 after the adoption of the Resolution on the Conference's strategic direction[4] in Tirana in 2019, which included a Policy Strategy. PSWG1 was tasked with delivering two specific actions from the Policy Strategy, namely:

1. To complete an analysis of current frameworks for privacy and data protection, including key principles, data subject rights, cross border transfers and demonstrable accountability standards.
2. To consider developing common definitions of key data protection terms.

PSWG1 delivered the frameworks analysis in 2019-20, and it was adopted as an annex to the PSWG1 annual report[5].

In 2020-21 PSWG1 worked on three specific topics leading on from the main analysis:

- Further analysis of cross border transfer mechanisms

  While the 2020 frameworks analysis found broad agreement across the frameworks in relation to the general principle of the need to protect personal data across borders, it found a variety of mechanisms in use. This further analysis surveyed GPA members as well as considering the frameworks to identify the mechanisms in use. The mechanisms were then analysed to identify areas of commonality.

- Key features of independent data protection authorities

  The 2020 analysis found that almost all of the ten frameworks analysed required or recommended the establishment of a supervisory or privacy enforcement authority. Eight out of the ten made specific reference to independence requirements of authorities. It was agreed that further work on the key features of independent authorities would be considered. This work has been carried out in 2021 and includes a more detailed analysis of the requirements set out in the frameworks, and a report, which recommended the development of a referential document.

- Government access to personal data

  PSWG1 committed to considering this topic in our 2020-21 forward plan, to follow on from the frameworks analysis where it was only briefly referred to in the section on scope. Work on this topic in 2021 has included a GPA member survey on the guarantees and safeguards member jurisdictions had in place to allow and frame government and public authority access to personal data held by the private sector

[4] Global Privacy Assembly, Resolution on the Conference's Strategic Direction 2019-21, adopted October 2019
[5] Global Privacy Assembly, Policy Strategy Working Group 1: Global frameworks and standards Annual Report, adopted October 2020

for national and public security purposes. A report has been produced and, at the time of writing, a draft resolution is being considered on the topic of government access to personal data and may be submitted for adoption at the October Closed Session.

To fulfil our second Policy Strategy action, PSWG1 also worked on:

- Common definitions of key data protection terms

  A report, analysis and initial list of key terms and their meanings have been produced.

All reports and outputs in relation to these topics can be found in annexes to this report.

The PSWG1 Chair attended a 'deep dive' meeting with the GPA ExCo's Strategic Direction Sub-Committee (SDSC) in March 2021. During this meeting a presentation was made to SDSC on progress made. Discussions focused on the continued need to engage externally and promote work done, which PSWG1 has worked on in 2021 and will focus on in 2021-22 and 2022-23.

Working Group members

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

Working Group Activities

Further analysis of cross border transfer mechanisms

While the 2020 frameworks analysis found broad agreement across the frameworks in relation to the general principle of the need to protect personal data across borders, it found a variety of mechanisms in use. PSWG1 therefore decided to carry out some further analysis on cross border transfer mechanisms in 2020-21.

The ten frameworks analysed in 2020 were considered again, this time with more focus on the mechanisms they provided for cross border data transfers. The African Union Convention on Cyber Security and Personal Data Protection did not include relevant provisions, so this framework was not included in the analysis. Instead, the Organisation of American States Principles on Privacy and Personal Data Protection – Eleventh Principle was included.

PSWG1 also surveyed GPA members in addition to considering the frameworks, to identify commonly-used mechanisms, or to identify any other mechanisms in use.

Mechanisms such as equivalence, contractual safeguards, self-assessment schemes, binding corporate rules, codes of conduct, certification, administrative arrangements, derogations and supervisory authority authorisation were considered. They were then analysed to identify areas of commonality.

Some recommendations for future work are being considered, and in 2021-22 PSWG1 may consult the GPA Reference Panel in that regard.

The report can be found at Annex A.

Key features of independent data protection authorities

The 2020 analysis found that almost all of the ten frameworks analysed required or recommended the establishment of a supervisory or privacy enforcement authority. Eight out of the ten made specific reference to independence requirements of authorities. It was agreed that further work on the key features of independent authorities would be considered. This work has been carried out in 2021 and includes a more detailed analysis of the requirements set out in the frameworks.

The ten frameworks from the 2020 analysis were analysed in more detail, and relevant provisions extracted. This was done in parallel with an academic review of existing work on the importance of independent authorities, and consideration of the GPA census results which were made available to members in May 2021. Many of the factors identified in the academic review were included in at least some of the frameworks, and while some

frameworks included more factors and more detail than others, there was broad agreement.

A report has been produced, which recommended the development of a referential document. The report and referential document can be found at Annexes B and C.

Government access to personal data

PSWG1 committed to considering this topic in our 2020-21 forward plan, to follow on from the frameworks analysis where it was only briefly referred to in the section on scope. The work is timely - the issue of disproportionate government and public authorities' access to personal data is currently on the agenda of several different international fora (OECD, Council of Europe, United Nations and also at the G7 and G20 level).

The work commenced in 2021 with the circulation of a GPA member survey on the guarantees and safeguards member jurisdictions had in place, and also on any shared values, principles and good practices relating to government and public authority access to personal data held by the private sector for national and public security purposes. The objective of the questionnaire was to highlight the key principles shared by GPA members, and to identify those principles that the GPA could advocate for, with regard to preventing disproportionate government or public authorities' access to personal data held by the private sector for national and public security purposes.

PSWG1 engaged with selected other multilateral and intergovernmental fora already working on the issue, in particular the OECD and the Council of Europe, which took part in the working group meetings and discussions. As other fora discuss international standards, the GPA's focus is slightly different, seeking to identify high level principles that could be advocated for by the GPA.

The questionnaire results were analysed and a report has been produced, which found that there did appear to be some common principles across different regions of the GPA that could be advocated for by authorities.

At the time of writing, a draft resolution is being considered on the topic of government access to personal data and may be submitted for adoption at the October Closed Session. It should be noted that the objective of the resolution would be to advocate for high level principles (such as clear legal basis, proportionality, redress and independent oversight) regarding access to data held by the private sector by governments. This would allow data protection authorities, as a community, to take part in the ongoing debate, make their voices heard, and express their views on the principles that should be provided for in legislation regarding access to data by governments.

The report and draft resolution can be found at Annexes D and E.

Common definitions of key data protection terms

Terms and their meanings are vitally important. The work of the GPA on global frameworks and standards in 2019-21 focused on identifying commonality in global and regional privacy and data protection frameworks and instruments. It is therefore important to understand what is meant by the key terms in those frameworks and instruments, and to identify where shared meanings exist across frameworks.

PSWG1's work on data protection terms and their meanings is intended to be a rolling project that will continue beyond 2021. In 2021 PSWG1 started by identifying a list of terms where definitions already exist in the frameworks. Those terms were analysed to identify any commonality. Next, high level, relatively simple definitions have been developed, with the intention that those definitions could be agreed on across the GPA, and across those who use the frameworks. It should be noted that the definitions developed as part of this work will not be legal definitions – the aim is for the definitions to be high level, simple and practical.

A report, analysis and initial list of key terms and their meanings have been produced. These can be found at Annex F.

External engagement

PSWG1 took steps to socialise and promote our work, starting with the 2020 analysis. A slide deck was developed to assist any GPA members who had the opportunity to discuss the work.

The analysis has proven to be a useful piece of work in its own right, with positive feedback received and several instances of external organisations referring to it while working on related issues, and GPA members using it as a reference when preparing discussions with and submissions to their governments. Most recently, the analysis has been referenced in the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[6], where it is recommended as a resource for data controllers to assess a third country for suitability for data transfers from the EU.

In 2021, PSWG1 has engaged externally with OECD, Council of Europe and the Global Direct Marketing Association on various elements of our government access and data protection terms work.

[6] 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, Version 2.0, adopted 18 June 2021

External engagement will continue to be a feature of PSWG1's work in 2021-23, as we focus on developing formalised relationships with other fora undertaking similar work, as per the draft GPA Strategic Plan 2021-23.

Forward looking plan 2021-2022

PSWG1 is pleased to see that the new draft GPA Strategic Plan 2021-23 recognises the importance of global frameworks and standards, and has allocated two broad actions to the group, which we note will be renamed the Global Frameworks and Standards WG.

The draft Plan 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.

In 2021-23 PSWG1 will therefore carry out work on the following:

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

  We anticipate that 2022 will see the foundational work in relation to this action carried out.

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

  Having noted in 2021 the work done by the OECD, and the interest shown by the G7, G20 and WTO in issue relating to data free flows with trust, there is clearly some opportunity to engage with others doing similar work. PSWG1 will request the GPA Reference Panel to provide input in identifying such opportunities.

In addition to work relating to the new Strategic Plan, PSWG1 will also:

- Continue with the next phase of work on data protection terms.

  In 2021-22 the focus will be on the meaning of terms relating to core data protection principles.

- Continue with work on cross border transfer mechanisms.

  As a starting point, this year's report and any recommendations will be considered. The GPA Reference Panel will be consulted on appropriate further work.

Conclusion

In the first two years of its existence, PSWG1 has delivered its allocated Policy Strategy actions, as well as several related actions:

- 2020 frameworks analysis
- Further analysis of cross border transfer mechanisms
- Analysis of key features of independent authorities
- Consideration of government access to personal data as a topic
- First phase of work on data protection terms, including a list of meanings.

As the renamed Global Frameworks and Standards Working Group, we look forward to continuing to progress the GPA's work in this area.

Annexes

Annex A: Report on cross border transfer mechanisms

Introduction

In October 2020, the GPA Policy Strategy Working Group 1 (PSWG1) adopted its annual working group report, which included an analysis of ten global frameworks for privacy and data protection from across all GPA regions. This analysis looked at the main aspects of these frameworks, including key principles, data subject rights, cross-border transfers and demonstrable accountability standards.

Whilst this analysis found that there was broad agreement across the frameworks in terms of key principles, core rights and other requirements, differences were noted in the ways in which these frameworks handled cross-border transfers. In particular, while there were broadly similar general principles round the need to protect personal data across borders, the analysis found that there was a variety of different mechanisms in use. It was therefore decided to conduct further analysis on these mechanisms to identify areas of commonality. This report presents that analysis.

The ten frameworks compared in this report are:

- Madrid Resolution - Section 15
- OECD Privacy Guidelines – Part Four
- APEC Privacy Framework
- Council of Europe Convention 108 – Chapter III and additional protocol ETS 181[7]
- Council of Europe Convention 108+ - Chapter III Article 14
- Standards for Personal Data Protection for Ibero-American States (IAS Standards) – Chapter V
- ECOWAS Act on Personal Data Protection – Article 36 (ECOWAS Act)
- EU data protection standards (General Data Protection Regulation GDPR – Chapter V, and the EUDPR[8])

[7] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (2001)

[8] "EUDPR" (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No

Note regarding UK and Gibraltar – The UK and Gibraltar are no longer EU member states. However, the transfer mechanisms within their domestic laws remain the same as the EU GDPR at this time. The UK has also been granted adequacy by the EU.

- UN Guidelines for the Regulation of Computerized Personal Data Files – Section on Transborder dataflows (The UN Guidelines)

- Organisation of American States (OAS) Principles on Privacy and Personal Data Protection – Eleventh Principle (the OAS principles)

These are the same frameworks as the analysis performed in 2020, except for the following changes:

- The African Union Convention on Cyber Security and Personal Data Protection is not included in this analysis, as it does not include any provisions relating to cross-border transfers; and

- The OAS principles have been added to the analysis as they do contain provisions relating to cross-border transfers.

As noted in the analysis conducted last year, all frameworks shared common principles relating to the cross-border transfer of personal data, in particular that transfers can take place if appropriate levels of protection are in place.

The working group also surveyed the transfer mechanisms contained within GPA members' domestic data protection regimes via a questionnaire sent out to members. 33 members responded to the questionnaire, of which only four had no specific provisions within their domestic law specifically regarding cross-border transfers.

Mechanisms

1. **Equivalence**

45/2001 and Decision No 1247/2002/EC) applies to EU institutions. There is general alignment between the EUDPR and GDPR, including Chapter V and the rules on transfers.

The idea of equivalence or adequacy (i.e. allowing the transfer of data between countries offering equivalent levels of protection) is present in eight of the 10 frameworks examined. However, the extent to which it is detailed varies significantly. A number of the frameworks also contain derogations, which are discussed at section 8 below.

The **Madrid Resolution** states that, as a general rule, cross-border transfers may be carried out when the State to which the data is transmitted affords, as a minimum, the level of protection provided [by the Resolution]. In this regard, it acts as a minimum baseline. The Resolution does not, however, provide any further guidance on how a recipient State's protection levels should be assessed. It would therefore be for any country to decide for itself whether the other State provides the level of protection specified by the Resolution.

Paragraph 17 of the **OECD Guidelines** states that OECD member countries should refrain from restricting transborder flows of personal data between themselves and other countries that substantially observe the guidelines. Like the Madrid resolution, this essentially means that the guidelines act as a minimum baseline level of protection. Again, the guidelines do not define what is meant by "substantially observe" in this context, so it would be for member states to decide themselves whether a recipient country does indeed substantially follow the guidelines. It is worth noting, however, that many national data protection laws are based on the OECD guidelines.

Although in its original form, **Convention 108** did not contain a concept of equivalency (other than free flow of data between C108 parties), the additional protocol ETS 181 adds an equivalency concept, stating that parties *"…shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer".* C108 therefore imagines free flow of data between Parties to the Convention, whilst requiring an adequate level of protection for transfers to countries that are not Parties. Again, how adequacy should be assessed is not defined.

Like C108, **Convention 108+** provides for free flows of data between Parties to the convention, on the basis that countries that are a party to the Convention will have an equivalent level of protection to each other, as laid out in the Convention. Restrictions to this free flow of data may be envisaged if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation. C108+ also allows data to be transferred to non-Party countries if those countries offer an "appropriate" level of protection. Whilst it is still up to individual States to decide whether a non-Party country offers an appropriate level of protection, C108+ provides more guidance on how this should be assessed, including what factors should be considered. These include the extent to which the principles of the Convention are met in the recipient country or organisation in-so-far as they are relevant to the transfer, and how the data subject is able

to defend their rights and access redress. This assessment can either be made for a particular transfer, or for a whole country or organisation, thereby permitting all transfers.

The **IAS Standards** allow transfers of personal data where the recipient has been acknowledged as having an appropriate level of protection of personal data by the transferring country, in accordance with its national legislation. Essentially, this provides for individual IAS members to set up their own equivalency processes. Such a decision can apply to the specific transfer, the recipient country as a whole, or particular sectors within the recipient county. The IAS Standards do not provide any further information on how any such adequacy system should work, however. Importantly, this provision appears to apply to any states to which data is transferred, whether they are IAS members or not. There appears to be no assumption of free flow of data between IAS members.

The **ECOWAS Act** states that a data controller shall only transfer personal data to a non-ECOWAS country where that country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data. It also requires the controller to inform its Data Protection Authority prior to any transfer or personal data to a third country. The ECOWAS Act therefore appears to provide for free flows of data between ECOWAS countries, whilst adequacy is the only mechanism that allows transfers to non-member countries. It does not provide any further guidance on how adequacy should be assessed or who is responsible for assessing adequacy.

The **GDPR** contains perhaps the most well-known and well-developed concept of equivalency with its third country adequacy process. Under this process, the framework of a third country (i.e. non-EU-members) is assessed by the EU Commission as to whether they offer adequate levels of protection to any personal data transferred from the EU. Adequacy is defined as a level of protection that is "essentially equivalent" to that provided in the EU. The adequacy assessment takes not only the recipient country's data protection laws into account, but also the legal system as a whole, including any other laws that may impact on data protection and the country's overall respect for the rule of law and human rights norms. An adequacy decision can apply to all processing operations, or only to some of them (a partial adequacy decision). Once a country has been deemed adequate, transfers can be made to this country as if they were being made to another EU member state. Adequacy decisions are periodically reviewed and can ultimately be revoked if circumstances in the country in question have changed. To date, 13 non-EU countries have been granted adequacy by the EU.

The **UN Guidelines** contain perhaps the simplest expression of the concept of equivalency, stating that *"When the legislation of two or more countries concerned by a transborder data flow offers more or less equivalent safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned."* It goes on to state that where there are no such reciprocal safeguards, limitations on the circulation of data may not be admitted unduly and only in so far as the protection of privacy demands.

This specific section of the guidelines is therefore seeking to preserve cross-border data flows rather than limit them.

The **APEC Privacy Framework** and **OAS Principles** did not contain a concept of equivalence or adequacy, perhaps reflecting their focus on enabling data flows between countries with different data protection systems. The APEC framework does, however, contain a different mechanism for ensuring consistent privacy protections in the form of the Cross-Border Privacy Rules (CBPR) system, which is discussed in section 3 of this report.

National legislation – The concept or equivalence or adequacy is present in 24 of the countries surveyed, with 14 of the non-GDPR states that responded to the questionnaire having some form of equivalency recognised in their national law. However, there was significant variation in terms of the way equivalency was assessed and/or validated, ranging from individual data controllers assessing adequacy, through to all transfers having to be authorised by the supervisory authority, and even to "adequate" countries. In addition, the scope of the equivalence or adequacy assessed varies across jurisdictions, ranging from all processing undertaken in a country to an individual organisation.

Findings – Whilst the concept of equivalence is present in eight out of the 10 frameworks, only the GDPR contains a fully developed and active adequacy process. Convention 108+ has potential to provide a more broadly applicable framework for cross border transfers than other more regionally focused frameworks. Although at this time a specific process for assessing whether a non-C108 country offers *"an appropriate level of protection"* is not specified, the development of an Evaluation and Follow Up mechanism to assess compliance with the modernised convention based on the request of any country or international organisation may provide this. At national level, the story was similar, with the concept of equivalence or adequacy being fairly common, but the way it was defined or assessed varying. Some countries, such as Japan, have an active adequacy process, and the UK is currently in the process of developing its own.

2. Contractual safeguards

In the absence of equivalence, contractual safeguards between the transferring and recipient organisation are another common tool used enable the cross-border flow of personal data. These essentially seek to extend the protections provided by the law of the transferring country to the recipient organisation in the country to which the data is being transferred**. Of the 10 frameworks assessed, seven contain either a specific reference to**

the use of contracts, or make more general reference to possible safeguards, which could include contracts.

The **Madrid Resolution** refers to "appropriate contractual clauses" as an example of how those guarantees could be provided when transferring data to States that do not afford the level of protection provided by the Resolution. The Resolution does not go on to provide any further detail on exactly how those clauses should be worded or what they must contain.

The **OECD Guidelines** state that Member countries should refrain from restricting transborder flows of personal data to countries that do not substantially observe the Guidelines where *"sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines"*. The supplementary explanatory memorandum to the Guidelines mentions *"contracts"* as one of the measures that a data controller could put in place. The Guidelines do not provide any further clarification of what such contracts should contain, but they do state that any measures taken (including contracts) need to be *"sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective"*.

The additional protocol to **C108,** ETS 181, adds provisions to C108 that allow transfers to non-adequate countries "*…if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found to adequate by the competent authorities according to domestic law".* Whilst it does not specify standard clauses, it does suggest that any clauses must be found adequate by a competent authority, which would suggest that standard clauses could be a way of achieving this.

C108+ allows for *"…ad-hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing."* This could therefore include contractual clauses, although again there is no specified mechanism or standard clauses at this time.

The **IAS Standards** allow transfers if the exporter and recipient sign contractual clauses or any other legal instrument that offers sufficient guarantees and that allows proving the scope of the treatment of the personal data, the obligations and responsibilities assumed by the parties, and data subject' rights. Whether the competent DPA may validate the contractual clauses or legal instruments is left to the member states to determine in their own national legislation.

The **GDPR** specifies standard contractual clauses (SCCs) as a transfer mechanism to non-adequate third countries. The EU commission has approved and published standard clauses that can be used without further authorisation. Supervisory authorities can also authorise ad hoc contracts and develop their own standard clauses that would have to be approved by

the EU Commission, as well as authorising ad-hoc contracts. The EU standard clauses are one of the most commonly used mechanisms by organisations subject to the GDPR for the transfer of personal data, since the system is well established.

Finally, the **OAS** principles refer to the use of contracts for transferring personal data, although no specific mechanism is outlined. I particular, it states that data controllers *"…must take reasonable measures to ensure personal data is effectively protected in accordance with these Principles, whether the data is transferred to third parties domestically or across international boundaries. They should also provide the individuals concerned with appropriate notice of such transfers, specifying the purposes for which the data will be used by those third parties. In general, such obligations should be recognized in appropriate agreements or contractual provisions…"*

National legislation – The use of contracts to provide protection to data being transferred was one of the largest areas of commonality between different national level legislation, with virtually all laws either explicitly mentioning them as a transfer mechanism or implying their use in more general terms. In virtually all cases, the purpose of the contract was to extend the protections of the law of the exporting country to the recipient data controller. Whether these contracts included standard clauses or were ad-hoc, and whether a review or authorisation from supervisory authorities were necessary, varied across jurisdictions. However virtually all were intended to place binding obligations on the exporting and importing data controller to treat the personal data with an appropriate level of protection.

Findings – The use of contractual provisions to enable the transfer of personal data appears to be extremely widespread and a major area of commonality amongst different data protection frameworks and national laws.

3. Self-assessment schemes

The **APEC Framework** includes the most well-developed self-assessment scheme, in the form of the APEC Cross Border Privacy Rules (CBPR) system. Under this system, organisations can assess their own policies and procedures against the APEC Framework. This assessment is then considered by an "accountability agent", which can be a public or private sector body (including national DPAs). Accountability agents must be approved by the APEC Joint Oversight Panel, and individual countries must decide whether to join the CBPR system. Currently, nine APEC economies are part of the CBPR system; Canada, Japan, Mexico, South Korea, Singapore, United States, Australia, Taiwan and the Philippines.

Convention 108+ states that the Convention Committee may develop or approve models of standardised safeguards, which could include self-assessment schemes. However, none have been developed at this time.

Finally, the **IAS Standards** state that transfers can take place if the exporter and recipient data controllers adopt a binding self-regulation scheme or an approved certification mechanism. No such schemes are specified however, and at the time of writing no such schemes appear to have been developed.

None of the other frameworks included reference to self-assessment schemes.

National legislation – Four of the countries surveyed are members of the CBPR system. Of those that aren't, one made specific reference to data controllers assessing their own compliance.

Findings – Self-assessment does not appear to be a particular area of commonality between the frameworks at this time, although comparisons are often drawn between the CBPR process and the GDPR Binding Corporate Rules system (see below). There may also possibly be some areas of commonality between the CBPR system and any future approved certification schemes under the GDPR, although to date, none of the latter have been developed with regards to international transfers as this is still a relatively new mechanism.

4. Binding Corporate Rules (BCRs)

Of the 10 frameworks, two made specific mention of BCRs or a similar mechanism.

The **Madrid Resolution** states that, where transfers are carried out within corporations or multi-national groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory. It does not set out a specific mechanism for this, however.

The **GDPR** also includes BCRs as a specific appropriate safeguard that can allow transfers to non-adequate third countries within a multi-national group of undertakings or enterprises. As with SCCs, the BCR system is well established. It requires multi-national organisations to submit their BCRs for approval by the competent supervisory authority within the EU. The supervisory authority will assess and decide whether to approve the BCRs, in accordance with the GDPR's consistency mechanism. It must communicate its draft decision to the European Data Protection Board (EDPB) which will issue its opinion. Once the BCRs have been finalised in accordance with this opinion, the supervisory authority will approve the BCR. To date, 140 BCRs have been approved, 136 of which were approved under the GDPR's

predecessor Directive 95/46/EC and carried over, and 6 of which have been approved under the GDPR itself.

Note on UK BCRs: Following the UK's exit from the EU in Jan 2020 and the end of the 'bridge period' provided for in the EU-UK Trade and Cooperation Agreement of Dec 2020, EU BCRs no longer provide a valid transfer mechanism for transferring personal data from the UK to non-adequate third countries. Instead, data controllers will need a separate UK BCR if they wish to rely on BCRs as a transfer mechanism. What previous EU BCR holders need to do to obtain a UK BCR depends on whether the ICO or another supervisory authority was the lead and whether the ICO had previously issued an authorisation (where the ICO was not the lead supervisory authority). More information can be found on the ICO's website[9].

The **OECD** guidelines mention BCRs as an existing mechanism for transfers, but do not elaborate further. **C108+,** the **IAS Standards**, and **OAS Principles** all refer to measures in general that could include BCRs, although they make no specific mention of them.

National legislation – Alongside the GDPR member states, a further 12 countries that answered the questionnaire allow transfers based on BCRs or take them into account when making a more general assessment of the appropriateness of measures that a data controller has put in place. This makes BCRs a relatively common transfer mechanism. This reflects the fact that many national laws require data exporters to put protections in place in more general terms, meaning that either contracts or BCRs could be used, depending on the relationship between the data exporter and importer.

Findings – As with standard contractual clauses, BCRs are an accepted way of transferring personal data in many the domestic laws surveyed. However, only two international frameworks make specific reference to them.

5. Codes of conduct

Three of the frameworks included terms that could include Codes of Conduct as a viable transfer mechanism, with only the **GDPR** containing a developed mechanism their use.

The **GDPR** includes approved codes as an appropriate safeguard for transfers to non-adequate third countries. The competent supervisory authority must approve any code, but compliance with it can then be monitored by a body that has appropriate expertise in relation to the subject-matter of the code. The monitoring body must be accredited for that purpose by the supervisory authority. For this mechanism to be used, data recipients in

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#bcr

third countries must make binding and enforceable commitments (via contract or other legally binging instruments) to apply the code.

The **IAS Standards** state that transfers can take place if the exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism. However, no specific mechanism is included, and it would ultimately be up to member states to implement.

The **OAS** principles encourage member states to develop codes of conduct, but do not elaborate further on this.

National legislation – Of the countries that are not members of (or substantially follow) the GDPR, only two use codes of conduct as a possible transfer mechanism, whilst one other has proposed them in its upcoming law. One GDPR country had introduced a code of conduct scheme. Whilst not specifically aimed at transfers, this scheme did include transfers as one of the factors to be considered when assessing compliance with the scheme.

Findings – Codes of conduct are not particularly prevalent outside the GDPR, and even within the GDPR they are still not commonly used. However, as they are a relatively new mechanism within the GDPR at least, they may become more prevalent as codes are developed and could be relevant to particular sectors or types of organisation. The GPA should therefore monitor the development of such codes and how commonly they may be used in the future.

6. Certification

As with Codes of Conduct, only the **GDPR** contains a developed mechanism for the use of certification schemes as a way of enabling cross-border transfers. Under this mechanism, certification schemes can act as an appropriate safeguard for transfers to non-adequate third parties. Certification is performed by certification bodies based on criteria set out by the competent supervisory authority or the EDPB. Certification bodies must be accredited by the competent supervisory authority, or by the member state's national accreditation body with additional requirements from the supervisory authority. Schemes can operate either within a country or across the whole EU. Certification must be used in conjunction with binding, enforceable commitments by the recipient in the third country to apply appropriate safeguards to the transferred data, and all controllers or processors remain liable under the GDPR; certification does not absolve them of this. Certification can be issued for a maximum of three years and can be withdrawn of the certified organisation no longer meets the required standards.

As mentioned above for Codes of Conduct, the **IAS Standards** state that transfers can take place if the exporter and recipient adopt a binding self-regulation scheme or an approved

certification mechanism. However no specific mechanism is included; again, this appears to be left to member states to implement.

The **APEC CBPR** system has, on the face of it, some similarities to approved certification mechanisms.

National legislation – Apart from the GDPR countries or those that substantially mirror GDPR, no country surveyed specifically mentioned certification as a possible transfer mechanism, although one has proposed it in its upcoming privacy law.

Findings – As with Codes of Conduct, certification is a relatively new mechanism under the GDPR and is not prevalent amongst either GDPR or none-GDPR countries. Again, the GPA may wish to monitor the development of certification mechanisms and whether they provide new areas of commonality with other mechanisms such as the APEC CBPR system.

7. Administrative arrangements

The **GDPR** provides that provisions inserted into administrative arrangements between public authorities or bodies, which include enforceable and effective rights for data subjects, can be an appropriate safeguard for transferring personal data to non-adequate third countries. Conceptually these are similar to SCCs or BCRs, in the sense that the recipient commits to treat data transferred to them in compliance with the transfer tool used. Legally binding and enforceable instruments between public authorities do not require any specific authorisation from a supervisory authority. Administrative arrangements between public authorities or bodies, which include enforceable and effective data subject rights do not necessarily have to be binding. However, they are always subject to authorisation from the competent supervisory authority.

As with contractual obligations, **C108+** allows for *"…ad-hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing."* This could therefore include administrative arrangements, although again there is no specified mechanism or standard clauses at this time.

The **IAS Standards** allow transfers to take place if the exporter offers sufficient guarantees for the treatment of personal data in the recipient country and the recipient proves compliance. This can be achieved by signed contractual clauses/other legal instrument that offers sufficient guarantees, so administrative arrangements could potentially fall within this. However, it is ultimately for individual states to decide how to implement such a mechanism.

National legislation – Administrative arrangements were not specifically mentioned in any of the responses from non-GDPR countries. However, it is likely that they could be used in some form in those countries that had more general requirements on data exporters to apply safeguards to the data, where those exporters are public authorities.

Findings – Administrative arrangements as a specific transfer tool do not appear to be particularly prevalent outside the GDPR. However, they so provide an important tool for public authorities to satisfy more general requirements to protect data that they are transferring across borders.

8. Derogations

The **Madrid Resolution** and **GDPR** both contain specific derogations from their transfers requirements for particular situations in which it may be necessary to make a transfer. Derogations for transfers necessary for the performance of a contract or the implementation of pre-contractual measures, reasons of important public interest and the protection of the data subject or another individual's vital interests were common between the two. The GDPR also includes derogations for transfers made as part of an open public register, for the establishment, exercise or defence of legal claims and transfers based on the explicit consent of the data subject.

C108 and C108+ both allow derogations to be made "for the specific prevailing interests of the data subject" or "legitimate prevailing interests, especially important public interests". This leaves significant space for parties to develop derogations that suit their own circumstances.

The **IAS Standards** do not include specific derogations but leave it up to member states to include them in their law if they see fit.

National legislation – Many the countries surveyed included derogations in their national laws for specific circumstances. These were largely similar to those in the GDPR and Madrid resolution, with some additions for situations such as protecting freedom of expression, mitigating adverse action against the data subject, law enforcement and intelligence service cooperation and transfers required by law or international agreements.

Findings – Whilst not all the international frameworks included derogations, they were common at national level, reflecting the fact that data protection law cannot always account for every circumstance that may arise in any legal system. However, as derogations should, by their nature, only apply in specific limited circumstances, they are unlikely to be suitable as the basis for regular transfers that facilitate the free flow of data.

9. Authorisation from supervisory authority

The **Madrid Resolution** recognises that national legislation may confer powers on supervisory authorities to authorise some or all of the international transfers falling within their jurisdiction before they are carried out.

The **IAS Standards** also recognises that supervisory authorities can authorise transfers under the terms of the national legislation applicable to the matter.

The **ECOWAS Act** requires the relevant supervisory authority to be notified of all transfers to ECOWAS adequate countries, although it does not require them to be authorised. As mentioned above, there is no mechanism for transfers to non-adequate countries.

Under the **GDPR,**

authorisation from the competent supervisory authority is needed in some specific cases. These are:

- when public authorities or bodies are using a non-binding administrative arrangement (Article 46(2) and (3);
- where a data controller is using ad hoc contractual clauses (i.e. not the approved SCCs) (Article 46(3));
- when using a BCR (Article 47); and
- if it is not possible to any of the listed appropriate safeguards in place or rely on one of the derogations, a transfer can take place to non-adequate third country if it is not repetitive, concerns only a limited number of data subjects, is necessary for compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has put in place what it considers to be suitable safeguards based on an assessment of all the circumstances of the transfer. In such cases, controller must inform supervisory authority and data subject of the transfer (although prior authorisation is not required) (Article 49).

National legislation – the legislation of five GPA members requires authorisation from the DPA: three required authorisation from the supervisory authority for transfers to non-adequate countries. Another two required all transfers to be authorised. In addition, the legislation of 12 GPA members although not requiring the specific transfer to be authorised, requires information to the authority (9 GDPR members and 3 non GDPR members). Finally,

one included authorisation as a mechanism of transfer, although not a requirement in any particular case.

Findings – It is relatively rare for all transfers to require the prior authorisation of the supervisory authority. Such a requirement may present a barrier to seamless cross-border data flows and a significant administrative burden to supervisory authorities, particularly where authorisation is on a transfer-by-transfer basis.

Conclusions

Conceptually, there are a number of areas of convergence between the different global and national frameworks mentioned above. In particular, the idea of equivalence, use of contractual clauses and BCRs to enable transfers was common to many of the global frameworks and common to a number of the national frameworks analysed. There remain differences between how they are implemented, with a number of frameworks mentioning these mechanisms but not including more detail on how they should be applied.

It is also possible that some of the newer mechanisms under the GDPR, such as the use of codes and approved certification schemes, may become more prevalent as they develop. This, in particular, may develop into an area of increased commonality between the GDPR and APEC CBPR system, which may be worth further comparison.

Overall, despite the lack of detail on how to apply the above mechanisms in practice in some of the international and national level frameworks looked at, they represent a relatively consistent set of tools that can be used to transfer personal data. Data controllers making cross-border transfers are likely to have experience in using at least one, if not more, of the above mechanisms to do so. Jurisdictions that are yet to implement a cross-border transfers framework, or a data protection framework more generally, may therefore find the above useful when looking to develop such a framework themselves that aligns with other such frameworks around the world.

Next steps

There are a number of areas identified in this report that could benefit from further consideration by the GPA. This includes the fact that the use of contracts and BCRs feature in a number of national and international frameworks, and potential commonalities between the GDPR's approved certification scheme mechanism and the APEC CBPR system. As a next step, 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. Such consideration may benefit from the input of the GPA's reference panel.

Annex B: Key features of independent data protection / privacy enforcement authorities: analysis and report

Key features of independent data protection / privacy enforcement authorities

Analysis and report

1. Introduction

In 2020 the Global Privacy Assembly's (GPA) Policy Strategy Workstream 1: Global Frameworks and Standards Working Group delivered an analysis of ten global data protection and privacy frameworks which was subsequently adopted at the 42nd GPA Conference.

The analysis identified a strong degree of commonality and convergence between the ten frameworks, and highlighted several core principles, rights and themes that indicated a broad acceptance of those elements as important privacy protections in the current global environment.

The existence of an independent supervisory or enforcement authority was one such core element. It was noted in the analysis report that "Almost all frameworks require or recommend the establishment of a supervisory or privacy enforcement authority. Varying levels of specification of duties and powers exist, however many frameworks set out that they should be adequately resourced and that they should have powers of investigation. Eight of the ten frameworks make specific reference to independence requirements of such authorities."[10]

For this reason, it was agreed that further analysis of the key features of independent privacy and data protection authorities should be considered.

In 2021 we have carried out that more detailed analysis. This analysis is intended to identify and further explore the commonalities between the features of independent authorities set out in the ten global frameworks. The results of the analysis are then used to produce a referential document that sets out those common key features. The referential document is aimed at an external audience, as more countries continue to develop privacy and data protection laws and establish the supervisory authorities that will regulate those subject to

[10] Global Privacy Assembly Policy Strategy Working Group 1: Global frameworks and standards, Report – adopted October 2020

them. It should be noted that the analysis and referential document **will not** be used for the purposes of the GPA's own internal procedures in assessing member applications.[11]

2. Methodology

Several publications and papers were used in some initial research, carried out in order to develop a background knowledge into the nature of independence in the privacy and data protection context, and to understand which criteria were relevant in relation to independence.

The ten global frameworks analysed in the 2020 work were then analysed again, this time for a more detailed comparison of the provisions relating to supervisory authorities and their independence. Key criteria relating to independence were extracted from each of the frameworks, and listed in a table in order to identify the most commonly occurring factors. The analysis table can be found in Appendix 1, and the ten frameworks analysed were:

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

Part 1 of Graham Greenleaf's working paper on the independence of data privacy authorities[12] was particularly helpful when extracting the criteria relating to independence, with a majority of the thirteen factors identified by Greenleaf as elements of independence being quite closely reflected in many of the frameworks analysed.

The 2020 GPA Census[13] was also consulted, to identify any additional relevant criteria relating to independence used in the survey.

[11] Information relating to the GPA's internal procedures can be found on the GPA website: Become A Member – Global Privacy Assembly

[12] Graham Greenleaf (2011), "Independence of data privacy authorities: International standards and Asia-Pacific experience," University of Edinburgh School of Law Working Paper No 2011/42

[13] A link to the 2020 GPA Census can be found here: GPA Census – Global Privacy Assembly

3. The importance of independence

Before turning to the detail of the analysis, it is worth pausing to consider the importance of independence in the context of privacy and data protection authorities. Whatever the detailed role, responsibilities and tasks of an authority may be, in order to carry out its privacy and data protection functions objectively and fairly and apply the law in a uniform and impartial manner, there is general agreement that the authority's independence is a fundamental requirement. If an authority is to make objective and unbiased decisions about the application of privacy and data protection law to public authorities, including governments, and to private sector organisations, it must have some degree of independence from them all.

While some texts do not address why independence is important in this context, some commentary exists. The EU Agency for Fundamental Rights and the Council of Europe note that "the independence of the supervisory authority and its members, as well as of staff from direct or indirect external influences, is fundamental in guaranteeing full objectivity when deciding on data protection matters."[14] The OECD in its Supplementary explanatory memorandum, where new provisions on privacy enforcement authorities were added to the privacy guidelines revised in 2013, referred to "the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy," "the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions," and added that the practical impact of mechanisms to ensure impartiality "should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity."[15] The Council of Europe, in its Explanatory Report to Convention 108+, emphasises the importance of independence and lists several elements contributing to it: "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient

[14] European Union Agency for Fundamental Rights and Council of Europe, 2018, Handbook on European data protection law

[15] OECD 2013, The OECD Privacy Framework, Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, p.28.

resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect."[16]

While there is general agreement that independence is a vital element of the nature and role of a supervisory authority, it is apparent from the quotes above that there are many factors that relate to the independence of authorities. The focus of this analysis is to identify those common factors in the ten framework texts, and the next section lists the more common factors identified.

4. Key features of independent authorities identified in global framework texts

On analysing the ten global frameworks, we found that while some frameworks included only high-level references to the independence of authorities, provisions in most frameworks listed several factors relating to independence. Those factors can be grouped into three main types: institutional independence, functional independence and material independence.

Institutional independence factors

- Requirement to establish a supervisory authority

Nine of the ten frameworks include a high-level requirement for a supervisory authority to be established, to be responsible for ensuring compliance with the requirements of the framework in questions. The APEC Privacy Framework does not include an explicit requirement but does suggest that "Member economies should consider establishing and maintaining Privacy Enforcement Authorities.."

- Supervisory authority should be impartial / independent

Eight of the ten frameworks include explicit reference to authorities being impartial and/or independent, or that they should act with independence and impartiality in exercising their powers and functions. The APEC Privacy Framework and the OECD Privacy Guidelines do not explicitly require that the authority is independent, instead requiring that authorities are provided with the necessary conditions to "make decisions on an objective, impartial and consistent basis."

- The appointment of the authority's members, their term of office and conditions for removal from office

All elements of this factor aim to contribute to ensuring the independence of the members of the supervisory authority. Four of the ten frameworks refer to the method of

[16] Council of Europe, June 2018, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, Explanatory Report to the Protocol amending the Convention for the protection of individuals with regard to the processing of personal data.

appointment of the authority's members as an important factor for independence. The Explanatory Report to Convention 108+ simply notes "the method for appointing its members" as a contributory element to safeguarding the supervisory authority's independence. The Ibero-American Standards require a transparent appointment process under national law, and the ECOWAS Supplementary Act requires each member state to take the "necessary measures to determine the membership of the data protection Authority." Finally, GDPR requires a transparent procedure and additionally specifies that the appointment be undertaken by parliament, government, head of state or an independent body entrusted with the appointment under Member State law.

A fixed term of office allows for stability of the authority's leadership, and when combined with specified and limited conditions for removal from office, prevents the arbitrary removal of heads and members of the authority, thus supporting independence. Two frameworks refer to term of office: the Explanatory Report to C108+ notes the duration of the term as a contributory factor to safeguarding the supervisory authority's independence. The other framework, GDPR, sets out that terms of office should be provided for in law, for a period of no less than four years. In addition law should also provide for whether, and if so for how many terms, a member of the supervisory authority is eligible for reappointment.

Finally, conditions for the removal from office of a member of the supervisory authority is referred to in three of the ten frameworks. As before, the Explanatory Report to C108+ simply notes this as a contributory factor to safeguarding the supervisory authority's independence. The Ibero-American Standards require that a member of the authority can only be removed due to serious causes set out in law. The GDPR sets out that a "member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties."

- Restrictions on authority members undertaking incompatible activities / freedom from conflicts of interest

This factor is also concerned with ensuring the independence of members of the authority. If authority members are also members of government, or hold positions or other interests in the businesses they regulate, the risk exists that those positions/activities may influence their judgement when applying the law, creating a conflict of interests.

While it may be surprising that only four frameworks directly mention this factor, the overarching requirement of independence in almost all frameworks could be interpreted to entail similar restrictions.

The OECD Supplementary explanatory memorandum sets out a general requirement, referring to the need for privacy enforcement authorities to be "free from instruction, bias or conflicts of interest when enforcing laws protecting privacy." Three other frameworks include more specific restrictions on authority members undertaking incompatible business or government activities: the African Union Convention is clear that "Membership of the

national protection authority shall be incompatible with membership of Government, carrying out the functions of business executive and ownership of shares in businesses in the information and communication technologies sector." GDPR is similarly clear, setting out that "Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not," and that "Each Member State shall provide by law […] the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office.." The ECOWAS Supplementary Act states that "Membership of the data protection Authority shall be incompatible with membership of government, the exercise of business executives, and ownership of shares in businesses in the information or telecommunications sectors."

- Immunity for opinions expressed in connection with the authority's functions/duties

This is another factor contributing to the independence of the authority's members – giving them freedom and reassurance to express opinions in connection with their duties, without fear of reprisal. Authorities' objective application of the law will, of course, require critical opinions, decisions and judgements to be made at times.

This factor can be found in only two frameworks: the African Union Convention states that **"**Without prejudice to national legislations, members of the national protection authority shall enjoy full immunity for opinions expressed in the pursuit, or in connection with the pursuit of their duties. Similarly, the ECOWAS Supplementary Act requires that "Members of the data protection Authority shall enjoy full immunity in respect of opinions expressed in the exercise of, or during the tenure of their function."

- Judicial oversight of decisions

At first glance, this factor may not be an obvious choice to support the independence of an authority – as it may result in an authority's decisions being overturned. Greenleaf's perspective on this factor is particularly helpful, where he states that: "I would argue that to allow appeals to a political body against the decisions of a DPA does lessen its independence, but to allow appeals to a judicial body on such administrative law grounds as the failure to take into account proper considerations, or the failure to act according to natural justice, does in fact help ensure that a DPA acts independently of improper outside pressures or considerations, and does exercise genuine independence rather than unchecked caprice."[17]

Judicial oversight of decisions can, therefore, support an authority to act independently. There is broad agreement on the importance of this factor – seven of the ten frameworks

[17] Graham Greenleaf (2011), "Independence of data privacy authorities: International standards and Asia-Pacific experience," University of Edinburgh School of Law Working Paper No 2011/42

include it, and the Ibero-American Standards in particular goes on to highlight "the compelling need for each Ibero-American State to have an independent and impartial control authority, which decisions can **only** be appealed by judicial control." (Author's emphasis.)

Functional independence factors

- The authority should be free from instructions in the performance of its tasks

This factor is linked to the conflict of interest and incompatible activities factor above, but is somewhat broader. For an authority to perform its tasks independently, that authority should not be subject to external interference, or take instructions from any external body. It is a commonly-found factor in the frameworks, with six of them including some sort of reference to being free from, or not seeking or accepting instructions from external sources. Convention 108+ qualifies this to the extent that authorities should be able to seek the advice of specialists where necessary, as long as the authority continues to exercise its own independent judgement.

- The authority should have sufficient powers

This factor could be considered to have a less direct effect on the independence of an authority, however if an authority does not have sufficient powers to investigate, intervene, or bring proceedings then it would need to rely on other bodies to undertake those tasks, which could affect its ability to perform its tasks independently.

Seven frameworks include this factor, with several of these going on to specify specific powers the authority should have, such as investigative powers (six), powers of intervention (five), power to bring legal proceedings (four), and power to bring matters to the attention of the judiciary (four).

- Requirement to report to the legislature and/or the public

Five frameworks include this factor. While some focus on the importance of this factor for transparency, the requirement to report publicly or to parliament can support independence by adding a level of scrutiny to the work carried out and decisions made.

Material independence factors

- The authority should have technical competence / expertise

This is an important factor if an authority is to be able to apply the law in increasingly complex technical circumstances, and to make considered and credible decisions about similarly complex matters. In enhancing the authority's understanding of complex matters, and avoiding undue reliance on external advice, this factor supports independence.

Eight of the frameworks include this factor, with five focusing on a requirement of general technical competence / expertise, and three more specifically on the qualifications and expertise of the heads and members of the authority.

- The authority should have adequate resources

To effectively perform its tasks, exercise its powers, and make objective , impartial and consistent decisions without the interference of external bodies, an authority requires adequate resources of its own. Seven of the frameworks include this requirement, with several specifying the need for adequate human, technical and financial resources, premises and infrastructure. The OECD Supplementary explanatory memorandum adds that resources should be "commensurate with the scale and complexity of data processing operations subject to their oversight," and Convention 108+ adds that the adequacy of resources should be kept under review.

- The authority should have the ability to hire and direct its own staff

Two frameworks specify this factor as a requirement, which supports independence by ensuring that the authority does not have externally-influenced staff imposed upon it, and that it can independently direct its own staff in order to perform its tasks.

- The authority should have appropriate control over its own budget

Two frameworks refer to the authority's budget. The ECOWAS Supplementary Act provides that the authority should receive a budget allocation from government. This implies that the authority would have its 'own' budget, which would in turn support independence by reducing the potential for external interference. GDPR is more explicit, setting out that "Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget."

5. Conclusion

It is positive that all the frameworks analysed include an independence requirement in most cases, and at least a recommendation or similar reference to the importance of independence.

In terms of the frequency of inclusion in the frameworks analysed, we can conclude that in addition to general, overarching requirements for authorities to be independent the following additional factors are commonly agreed to be important:

- The authority should be free from instructions in the performance of its tasks
- The authority should have technical competence / expertise
- The authority should have adequate resources

- The authority should have sufficient powers
- Judicial oversight of decisions
- Requirement to report to the legislature and/or the public

The less commonly stipulated factors were:

- The appointment of the authority's members, their term of office and conditions for removal from office
- Restrictions on authority members undertaking incompatible activities / freedom from conflicts of interest
- Immunity for opinions expressed in connection with the authority's functions/duties
- The authority should have the ability to hire and direct its own staff
- The authority should have appropriate control over its own budget

While it may be surprising that some of the factors in the latter list are less commonly stipulated, this can be interpreted in two ways. It could be that these factors are not seen as so important to ensuring independence. Alternatively, the reason could be that all the frameworks have at least some degree of an overarching requirement for authorities to be independent, and that requirement could be interpreted to in turn entail any number of the less-commonly stipulated factors. While this analysis has not investigated to any depth which interpretation might be correct, it is interesting to note the following:

- The OECD Supplementary explanatory memorandum notes that "There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions."[18] It goes on to state that the guidelines focus on the practical impact of those mechanisms, implying their importance even though they are not listed.
- The Council of Europe, in its Explanatory Report to Convention 108+, lists several elements contributing to independence, including some of those elements from the list above, of those not so commonly specified in all the frameworks ("..the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; [...] the possibility to hire

[18] OECD 2013, The OECD Privacy Framework, Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, p.28.

its own staff;"[19] It is significant that these elements feature in the more general overarching frameworks.

- The GPA Census shows the importance of some of these elements in practice. For example, most authorities were allocated funding from their respective governments, indicating that authorities do tend to have their own budgets under their control. It is also apparent from the Census that procedures for appointing heads of authority had seen an increase in appointment by the executive, but also an increase in appointment by legislative committee, and a decrease in appointment by direct hire/civil servant and by 'other' methods, indicating the importance of the method of appointment of authority members.

It is therefore proposed that a referential document is produced, highlighting the importance of independence and listing the broadly agreed factors found in the analysis. It is also proposed that the less commonly stipulated factors should also be included in the referential document, with appropriate weighting and caveats, for the reason set out above.

6. References:

African Union (2014) *African Union Convention on Cyber Security and Personal Data Protection*. Available at African Union Convention on Cybersecurity and Personal Data Protection • Page 1 • ICT Policy Africa

Asia-Pacific Economic Cooperation (2015) *APEC Privacy Framework (2015).* Available at APEC Privacy Framework (2015)

Council of Europe (1981) *Treaty No. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Available at Full list (coe.int)

Council of Europe (2001) *Treaty No. 181: Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*. Available at Full list (coe.int)

Council of Europe (2018) *Convention 108+ Convention for the protection of individuals with regard to the processing of personal data.* Available at 16808b36f1 (coe.int)

[19] Council of Europe, June 2018, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, Explanatory Report to the Protocol amending the Convention for the protection of individuals with regard to the processing of personal data.

Economic Community of West African States (2010) *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS*. Available at ecowas-dp-act.pdf (statewatch.org)

European Union Agency for Fundamental Rights (2012) *Elements of independence of the data protection authorities in the EU: Data Protection authorities' funding and staffing*. Available at Elements of independence of data protection authorities in the EU (asktheeu.org)

European Union Agency for Fundamental Rights and Council of Europe (2018) *Handbook on European data protection law.* 2018 edn. Available at Handbook on European data protection law (europa.eu)

Global Privacy Assembly (2009) *International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution.* Available at 14302 STANDARS.qxp:Maquetación 1 (globalprivacyassembly.org)

Global Privacy Assembly (2019) *Working Group on the Future of the Conference Interpretation of the Autonomy and Independence Criteria*. Available at ICDPPC - Background document on independence criteria (globalprivacyassembly.org)

Global Privacy Assembly (2020) *Policy Strategy Working Group 1: Global frameworks and standards Report – adopted October 2020*. Available at Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf (globalprivacyassembly.org)

Greenleaf, G (2011) *Independence of data privacy authorities: International standards and Asia-Pacific experience.* University of Edinburgh School of Law Working Paper No 2011/42. Available at Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience by Graham Greenleaf :: SSRN

OECD (2013) *The OECD Privacy Framework* Available at Microsoft Word - Modernising priv framework.docx (oecd.org)

Red Iberoamericana de Proteccion de Datos (2017) *Standards for Personal Data Protection for Ibero-American States.* Available at Portada RIPD ing (dataguidance.com)

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2016. Available at CL2016R0679EN0000020.0001.3bi_cp 1..1 (europa.eu)

United Nations (1990) *Guidelines for the Regulation of Computerized Personal Data Files*. Available at Guidelines for the Regulation of Computerized Personal Data Files (refworld.org)

Appendix 1: Table of criteria relating to the independence of authorities identified in the framework texts

Criterion	**Identified extracts from framework texts (emphasis added)**
Requirement for a supervisory authority (9, with 1 implicit reference)	**Madrid: "**in every State there will be one or more supervisory authorities, in accordance with its domestic law.." **OECD:** "In implementing these Guidelines, Member countries should […] establish and maintain privacy enforcement authorities.." **APEC: (**No explicit requirement). "Member economies should consider establishing and maintaining Privacy Enforcement Authorities.." **C108 Additional Protocol:** "Each party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law.." **C108+:** "Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention." Explanatory Report: [Supervisory authorities] "are an essential component of the data protection supervisory system in a democratic society."

	Ibero-American Standards: "**Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority**, which decisions can only be appealed by judicial control, free of any external influence, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions;" "There **must be one or more control authorities on personal data protection in each Ibero-American State, with full autonomy**, in accordance with their applicable national legislation." **African Union Convention:** Each State Party shall establish an authority in charge of protecting personal data. […] **The national protection authority shall be an independent administrative authority** with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention.

	GDPR: "**Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation."** "Each Member State shall **provide by law […] the establishment of each supervisory authority**." **UN Guidelines:** "The **law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles**.." **ECOWAS Supplementary Act:** "Within the ECOWAS space, **each Member State shall establish Its own data protection Authority. Any State that does not have shall be encouraged to establish one**."
Authority must be impartial / independent (8, with 2 implicit references)	**Madrid: "**These supervisory authorities shall be **impartial and independent**.." **OECD: (**No explicit requirement.) "In implementing these Guidelines, Member countries should […] establish and maintain privacy enforcement authorities with the governance, resources

	and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, **impartial** and consistent basis." **APEC:** (No explicit requirement.) "Privacy Enforcement Authorities that are established should be provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, **impartial** and consistent basis." **C108 Additional Protocol:** "The supervisory authorities shall exercise their functions in **complete independence**." **C108+:** "The supervisory authorities shall act with complete **independence and impartiality** in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions." **Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in **complete independence**. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition

	of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect. **Ibero-American Standards:** "**Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority**, which decisions can only be appealed by judicial control, free of any external influence, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions;" "Control authorities may be single-member or multiple-member bodies; **they shall act impartially and independently in their jurisdictions**, and they shall be free or any external influence, whether direct or indirect, and they shall not request nor admit any order or instruction."

	African Union Convention: The national protection authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention. **GDPR:** "Each supervisory authority **shall act with complete independence** in performing its tasks and exercising its powers in accordance with this Regulation." **UN Guidelines:** "This **authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data**, and technical competence." **ECOWAS Supplementary Act**: "The data protection Authority **shall be an independent administrative Authority** responsible for ensuring that personal data is processed in compliance with the provisions of this Supplementary Act."

Authority must be free from instructions, bias or conflicts of interest (6, with 3 adding specific restrictions on authority members undertaking incompatible business or government activities, and 1 making a general reference to the need to be free from conflicts of interest)	**OECD Supplementary explanatory memorandum:** [The provision that Member countries should establish privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis] "..refers to the need for privacy enforcement authorities to be **free from instructions, bias or conflicts of interest** when enforcing laws protecting privacy." **C108+:** "The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so **shall neither seek nor accept instructions**." **Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or

	the adoption of decisions **without being subject to external interference, whether direct or indirect**. "The prohibition on seeking or accepting instructions covers the performance of the duties as a supervisory authority. This does not prevent supervisory authorities from seeking specialised advice where it is deemed necessary as long as the supervisory authorities exercise their own independent judgment." **Ibero-American Standards:** "Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority, which decisions can only be appealed by judicial control, **free of any external influence**, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions;" "Control authorities may be single-member or multiple-member bodies; they shall act impartially and independently in their jurisdictions, and **they shall be free of any external influence, whether direct or indirect, and they shall not request nor admit any order or instruction.**

	African Union Convention: "Membership of the national protection authority shall be incompatible with membership of Government, carrying out the functions of business executive and ownership of shares in businesses in the information and communication technologies sector. **"**Members of the national protection authority **shall not receive instructions from any other authority** in the performance of their duties. **GDPR:** " The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain **free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody**." "Member or members of each supervisory authority shall **refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not."** "Each Member State shall **provide by law […] the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations**

	and benefits incompatible therewith during and after the term of office.." **ECOWAS Supplementary Act:** "Membership of the data protection Authority shall be **incompatible with membership of government, the exercise of business executives, and ownership of shares in businesses in the information or telecommunications sectors**. "Members of the data protection Authority […] **shall receive no instructions from any Authority In discharging their duties**."
Authority must have technical competence / expertise (8, with 5 of these referring to general technical competence and expertise within the authority, and 3 of these focusing specifically on the qualifications of members / heads of authority)	**Madrid: "**These supervisory authorities shall be impartial and independent, and **will have technical competence**, sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data." **OECD:** [Members should] "establish and maintain privacy enforcement authorities with the […] **technical expertise** necessary

	to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." **Supplementary explanatory memorandum:** [**technical expertise**] "has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background." **APEC:** "Privacy Enforcement Authorities that are established should be provided with the governance, resources and **technical expertise** necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." **C108+ Explanatory Report:** "The supervisory authorities should have the necessary infrastructure and financial, **technical and human resources (lawyers, IT specialists)** to take prompt and effective action." "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority;

	the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; **the option to consult technical or other experts or to hold external consultations;** the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect. **Ibero-American Standards: The member or members of the direction bodies of the control authorities must have the necessary experience and skills, especially with respect to the field of personal data protection, for compliance with their functions and the exercise of their powers.** They shall be appointed through a transparent procedure under applicable national legislation and may only be removed due to serious causes, established in the internal law of each Ibero-American State, according to the rules of due process. **GDPR:** "Each member shall have the **qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers**.

	"Each Member State shall **provide by law […] the qualifications and eligibility conditions required to be appointed as a member if each supervisory authority**." **UN Guidelines:** "This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and **technical competence**." **ECOWAS Supplementary Act**: "This Authority must be composed of **qualified persons in the field of law, information communication technology and any other field of knowledge to achieve the objectives** defined in Article 2 of this Supplementary Act.
Authority must have sufficient powers (7, with several specific powers referred to: investigative (6), intervention (5), bring legal proceedings (4), bring to the attention of the judiciary (4), as well as less frequent references to powers of authorisation and advice, and audit.)	**Madrid: "**These supervisory authorities shall be impartial and independent, and will have technical competence, **sufficient powers** and adequate resources to deal with the claims filed by the data subjects, and **to conduct investigations and interventions where necessary** to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data."

	OECD (**Supplementary explanatory memorandum):** "privacy enforcement authority" refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, **provided they have the powers to conduct investigations or bring proceedings in the context of enforcing "laws protecting privacy"**. **C108 Additional Protocol:** "..the said authorities shall have, in particular, **powers of investigation and intervention**, as well as the **power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations** of provisions of domestic law giving effect to the principles.." **C108+:** "..such authorities […] shall have **powers of investigation and intervention** […] shall have **powers to issue decisions** with respect to violations of the provisions of this Convention {…} shall have the **power to engage in legal proceedings or to bring to the attention of the competent judicial authorities** violations of the provisions of this Convention."

	Ibero-American Standards: "Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority, which decisions can only be appealed by judicial control, free of any external influence, **with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter**, which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions;" "The applicable national legislation of the Ibero-American States **must grant the control authorities sufficient investigation, supervision, resolution, promotion, sanction and other powers that are necessary** in order to guarantee effective compliance with it, as well as the exercise and respect of the right to the protection of personal data. **GDPR: Article 58 Powers** includes "Each supervisory authority shall have the following […] "**investigative powers**".. .."**corrective powers**".. .."**authorisation and advisory powers**".. .."the **power to bring infringements of this Regulation to the attention of the judicial authorities** and, where appropriate, **to commence or engage otherwise in legal proceedings**."

	ECOWAS Supplementary Act: "The Data Protection Authority shall […] "**authorize** the processing of files".. .."**immediately inform the judicial authority** of certain types of offences".. .."**impose administrative and financial sanctions**".. .."**advise** individuals and bodies who process personal data".. .."issue […] a **warning** to a data controller who does not comply with the obligations".. "a **formal demand to desist** from the violations.."
Authority must have adequate resources (7)	**Madrid:** "These supervisory authorities shall be impartial and independent, and will have technical competence, sufficient powers and **adequate resources** to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data." **OECD:** "members should establish and maintain PEAs with the governance, **resources** and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." **Supplementary explanatory memorandum** "The **resources** of privacy enforcement authorities should be commensurate with the

	scale and complexity of data processing operations subject to their oversight." **APEC:** "Privacy Enforcement Authorities that are established should be provided with the governance, **resources** and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." **C108+:** "Each Party shall ensure that the supervisory authorities are provided with the **resources necessary** for the effective performance of their functions and exercise of their powers. **Explanatory Report:** "The **adequacy of resources** should be kept under review." "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to

	hold external consultations; **the availability of sufficient resources to the authority;** the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect. **Ibero-American Standards:** "Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority, which decisions can only be appealed by judicial control, free of any external influence, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, **which must be granted sufficient human and material resources in order to guarantee the exercise of its powers and the effective performance of its functions**;" "Control authorities **must have the necessary human and material resources** for complying with their functions." **African Union Convention:** " State Parties shall undertake to provide the national protection authority with the **human, technical and financial resources necessary to accomplish their mission**.

	GDPR: "Each Member State shall ensure that each supervisory authority is provided with the **human, technical and financial resources, premises and infrastructure necessary** for the effective performance of its tasks and exercise of its powers."
Appointment of the authority's members (4)	**C108+ Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; **the method for appointing its members;** the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect. **Ibero-American Standards:** The member or members of the direction bodies of the control authorities must have the necessary experience and skills, especially with respect to the field of personal data protection, for compliance with their functions and the

	exercise of their powers. **They shall be appointed through a transparent procedure under applicable national legislation** and may only be removed due to serious causes, established in the internal law of each Ibero-American State, according to the rules of due process. **GDPR:** "Member States shall provide for each member of their supervisory authorities to be **appointed by means of a transparent procedure by**: - their parliament; - their government - their head of state - an independent body entrusted with the appointment under Member State law. "Each member shall have the **qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers**. "Each Member State shall **provide by law […] the qualifications and eligibility conditions required to be appointed as a member if each supervisory authority**. […] **the rules and procedures for the**

	appointment of the member or members of each supervisory authority." **ECOWAS Supplementary Act:** "Each Member State shall **take necessary measures to determine the membership of the data protection Authority. This Authority must be composed of qualified persons in the field of law, information communication technology and any other field of knowledge** to achieve the objectives defined in Article 2 of this Supplementary Act." -
Term of office (2)	**C108+ Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; **the duration of exercise and conditions of cessation of their functions;** the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect."

	GDPR: "The **duties of a member shall end in the event of the expiry of the term of office**, resignation or compulsory retirement, in accordance with the law of the Member State concerned. "Each Member State shall **provide by law […] the duration of the term of the member or members of each supervisory authority of no less than four years […] whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment** ."
Removal from office (3)	**C108+ Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; **the duration of exercise and conditions of cessation of their functions;** the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect."

	Ibero-American Standards: "The member or members of the direction bodies of the control authorities must have the necessary experience and skills, especially with respect to the field of personal data protection, for compliance with their functions and the exercise of their powers. They shall be appointed through a transparent procedure under applicable national legislation and **may only be removed due to serious causes, established in the internal law of each Ibero-American State, according to the rules of due process."** **GDPR: "**A member shall be **dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties**."
Ability to hire its own staff (2)	**C108+ Explanatory Report:** "..supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue

	restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; **the possibility to hire its own staff;** or the adoption of decisions without being subject to external interference, whether direct or indirect." **GDPR:** "Each Member State shall ensure that **each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned**."
Immunity for opinions expressed in connection with duties / functions (2)	**African Union Convention: "**Without prejudice to national legislations, members of the national protection authority shall enjoy **full immunity for opinions expressed in the pursuit, or in connection with the pursuit of their duties**. **ECOWAS Supplementary Act:** "Members of the data protection Authority shall enjoy **full immunity in respect of opinions expressed in the exercise of, or during the tenure of their function**."

Judicial oversight of decisions (7)	**Madrid:** "In any case, without prejudice to any administrative remedy before the supervisory authorities referred to in the preceding paragraphs, **including judicial oversight of their decisions**, data subjects may have a direct recourse to the courts to enforce their rights under the provisions laid down in the applicable national legislation." **C108 Additional Protocol:** "Decisions of the supervisory authorities, which give rise to complaints, **may be appealed against through the courts**." **C108+:** "Decisions of the supervisory authorities **may be subject to appeal through the courts**." **Ibero-American Standards:** "Admitting the compelling need for each Ibero-American State to have an independent and impartial control authority, **which decisions can only be appealed by judicial control,** free of any external influence, with supervision and investigation powers on personal data protection, and in charge of supervising compliance with national legislation on the matter, which must be granted sufficient human and material resources in

	order to guarantee the exercise of its powers and the effective performance of its functions;" **African Union Convention:** "The **sanctions imposed and decisions taken by national protection authorities are subject to appeal**." **GDPR: Article 78 Right to an effective judicial remedy against a supervisory authority** "1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have **the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them**. **2.** Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

	3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established. **ECOWAS Supplementary Act:** The sanctions and decisions of the Data Protection Authority **may be subject to appeal**.
Requirement to report to the public / legislature (5)	**APEC:** Member economies should "Encourage or require Privacy Enforcement Authorities […] to **report publicly on their activities** where appropriate." **C108+:** "Each supervisory authority shall prepare and **publish a periodical report outlining its activities**." Explanatory Report: "..it seems particularly important that the supervisory authority proactively ensures the visibility of its activities, functions and powers. To this end, the supervisory authority must **inform the public through periodical reports**." "Transparency on the work and activities of the supervisory authorities is required […] through, for instance, **the publication of**

	annual activity reports comprising inter alia information related to their enforcement actions." **African Union Convention:** "The national protection authorities […] are responsible for […] Preparing an **activity report in accordance with a well-defined periodicity, for submission to the appropriate authorities of the State Party**." **GDPR: Article 59 Activity Reports** "Each supervisory authority shall draw up an **annual report on its activities**, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those **reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.** **ECOWAS Supplementary Act:** "The Data Protection Authority shall […] draft an **activity report** according to a well defined schedule, **for submission to the President of the Republic or the Speaker of the National Assembly, the Prime Minister, or the Minister of Justice"**

Independent budget (2)	**GDPR:** Each Member State shall ensure that each supervisory authority is subject to **financial control which does not affect its independence and that it has separate, public annual budgets**, which may be part of the overall state or national budget. **ECOWAS Supplementary Act:** "The data protection Authority shall receive a budget allocation from government to enable it to carry out its missions."

Annex C: Referential document on the key features of independent authorities

REFERENTIAL DOCUMENT ON THE KEY FEATURES OF INDEPENDENT AUTHORITIES

The importance of independence

Whatever the detailed role, responsibilities and tasks of an authority may be, in order to carry out its privacy and data protection functions objectively and fairly and apply the law in a uniform and impartial manner, there is general agreement that the authority's independence is a fundamental requirement. If an authority is to make objective and unbiased decisions about the application of privacy and data protection law to public authorities, including governments, and to private sector organisations, it must have some degree of independence from them all.

The key features of independent authorities

Institutional independence factors

- **A requirement to establish a supervisory authority**

It is important for a supervisory authority to be established, to be responsible for monitoring compliance with the requirements of data protection and privacy in the relevant jurisdiction.

- **The supervisory authority should be impartial / independent**

This is important so that the authority can make decisions on an objective, impartial and consistent basis.

- **The appointment of the authority's members, their term of office and conditions for removal from office**

All elements of this factor aim to contribute to ensuring the independence of the members of the supervisory authority. The method of appointment of the authority's members is an important factor in safeguarding an authority's independence. This should involve transparent procedures undertaken by an appropriate body.

A fixed term of office allows for stability of the authority's leadership, and when combined with specified and limited conditions for removal from office, prevents the arbitrary removal of heads and members of the authority, thus supporting independence.

Finally, appropriate conditions for the removal from office of a member of the supervisory authority are important to safeguard the authority's independence. Examples of appropriate conditions could be set out in law, or could relate to serious misconduct, or if the member no longer fulfils the conditions required fir the performance of their duties.

- **Restrictions on authority members undertaking incompatible activities / freedom from conflicts of interest**

This factor is important to safeguard the independence of members of the authority. If authority members are also members of government, or hold positions or other interests in the businesses they regulate, the risk exists that those positions/activities may influence their judgement when applying the law, creating a conflict of interests.

- **Immunity for opinions expressed in connection with the authority's functions/duties**

This is another factor contributing to the independence of the authority's members – giving them freedom and reassurance to express opinions in connection with their duties, without fear of reprisal.

- **Judicial oversight of decisions**

Appeals to a judicial body on administrative law grounds can to help ensure that a DPA acts independently of improper outside pressures or considerations, therefore supports independence.

Functional independence factors

- **The authority should be free from instructions in the performance of its tasks**

This factor is linked to the conflict of interest and incompatible activities factor above, but is somewhat broader. For an authority to perform its tasks independently, that authority should not be subject to external interference, or take instructions from any external body.

- **The authority should have sufficient powers**

This factor could be considered to have a less direct effect on the independence of an authority, however if an authority does not have sufficient powers to investigate, intervene, or bring proceedings then it would need to rely on other bodies to undertake those tasks, which could affect its ability to perform its tasks independently.

- **Requirement to report to the legislature and/or the public**

Also important for transparency, a requirement to report publicly or to parliament can support independence by adding a level of scrutiny to the work carried out and decisions made.

Material independence factors

- **The authority should have technical competence / expertise**

This is an important factor if an authority is to be able to apply the law in increasingly complex technical circumstances, and to make considered and credible decisions about similarly complex matters. In enhancing the authority's understanding of complex matters, and avoiding undue reliance on external advice, this factor supports independence.

- **The authority should have adequate resources**

To effectively perform its tasks, exercise its powers, and make objective , impartial and consistent decisions without the interference of external bodies, an authority requires adequate resources of its own.

- **The authority should have the ability to hire and direct its own staff**

This factor supports independence by ensuring that the authority does not have externally-influenced staff imposed upon it, and that it can independently direct its own staff in order to perform its tasks.

- **The authority should have appropriate control over its own budget**

This supports independence by reducing the potential for external interference.

Annex D: Analytical report on the GPA's questionnaire on government access to personal data

GPA – PSWG1 – ANALYTICAL REPORT

BACKGROUND

The issue of disproportionate government and public authorities' access to personal data has become a relevant topic and is now on the agenda of different international fora (OECD, Council of Europe, United Nations and it also had been addressed at the G7 and G20 level, in particular within the context of the initiative on "Data Free Flow with Trust").

In line with our commitment in taken at the 2020 Closed Session in Tirana to make the GPA a policy leader at the global level, the new Policy Strategy Working Group 1 ("PSWG 1") highlighted in 2019-2020 a need to identify key principles and common standards shared among data protection frameworks. At the end of the year, the adopted PSWG1's forward plan suggested that, in the context of that work, further consideration should be given to the issue of guarantees against disproportionate government and public authorities' access to personal data.

As a first step, the working group tasked with following up on this initiative has prepared a questionnaire to understand whether and which values and principles are shared on this topic among data protection authorities.

The main purpose of this exercise was not to identify a common denominator based on existing legal principles but rather to gain knowledge and overview on key concepts shared among GPA members across different regions of the world.

Then as a second step, it was agreed that CNIL France, OPC Canada and PPC Japan, with the support of Policy Strategy Working Group 1, would propose a new workstream summarized in a draft resolution to the GPA members for comment and eventual adoption at the next GPA closed session to be held in Mexico on 20-21 October. In developing this workstream, PSWG1 has engaged with selected other multilateral and intergovernmental fora already working on the issue, in particular the OECD and the Council of Europe, which took part in the working group meetings and discussions.

OBJECTIVE

While international standards on this important issue are currently under discussion in various fora, the objective of the GPA paper is to advocate for high level principles (such as clear legal basis, proportionality, redress and independent oversight) regarding access to data held by the private sector by governments.

In other words, the objective is to highlight the key principles we share or we can advocate for with regard to preventing disproportionate government or public authorities' access to personal data held by the private sector for public security and national security purposes, and not to identify a common denominator based on existing legal principles.

The adoption of a policy paper on this issue – which could possibly take the form of a statement or a resolution - would allow data protection authorities, as a community, to take part in the ongoing debate, make their voices heard, and express their views on the principles that should be provided for in legislations regarding access to data by governments.

TIMELINE

At the PSWG1 meeting, on November 24 2020, the draft work plan for 2020-21 was agreed. The adopted forward plan suggested that further consideration should be given to the issue of government and public authority access to personal data. Working group members shared their views on how this topic could be addressed. It was agreed that since Data Protection Authorities ("DPAs") are key stakeholders, the GPA should consider whether to issue a deliverable on this important issue to ensure that DPAs are part of the discussion. As an initial proposal, it was considered to draft a questionnaire to understand whether shared values between DPAs exist. Some of the working group members volunteered to follow-up this work item.

A sub-group meeting was organized on January 13 2021, gathering the volunteering working group members (ICO/Secretariat, Council of Europe, CNIL France, Philippines, Switzerland FDPIC, and OECD Observer). An initial draft of the questionnaire prepared by CNIL France was discussed between the sub-group members. Some changes were agreed and it was decided that a revised version of the questionnaire will be shared with this sub-group and then with the wider PSWG1 to agree at the whole working group meeting on 27 January.

At the PSWG1 meeting, on January 27 2021, the revised version of the updated draft questionnaire was presented and a discussion took place between working group members. It was agreed to remove a question and that the scope of the questionnaire could be reduced to target access for national and public security purposes only.

Then, the final version of the questionnaire was circulated to PSWG1's members for written comments.

On February 24 2021, the questionnaire was circulated to GPA members. The members had until 22 March 2021 to address their answers to the GPA Secretariat.

At the PSWG1 meeting, on April 21 2021, the CNIL gave a brief presentation on the initial analysis of the responses to the questionnaire on government access to personal data held by the private sector. The interim results, based on the answers received so far, were discussed at subgroup level. There did appear to be some common principles, and a brief discussion was had as to whether a resolution or declaration setting out member authorities' recommended principles should be drafted and submitted to the closed session.

It was agreed that discussions should continue after the analysis of the results will be completed.

At the PSWG1 meeting, on July 4 2021, it was agreed that CNIL France, OPC Canada and PPC Japan would propose a draft resolution to the membership, underlining those key values which could help to frame government access. This "draft resolution for early consideration", to get feedback from the membership on the draft resolution and the workstream it proposes, was sent on July 16 2021. There will be then two other rounds of comments from 16 August to 10 September and from 20 September to 1 October on new versions based on comments received, before the final version is submitted for adoption at the closed session.

PRESENTATION OF THE QUESTIONNAIRE

The questionnaire includes four questions, one of which being divided into seven sub-questions. A template of the questionnaire can be found in Appendix 1.

The first question deals with the main guarantees, the second is about the competent supervisory authorities, the third deals with transparency reports, the fourth with any other guarantees that may be included in national legislations on this topic.

The aim of the exercise was not to conduct a benchmark analysis of existing legal principles to find common denominators but rather to find out whether there was general observance and/or agreement with the emerging principles at the international level related to the issue of government access.

PRESENTATION OF THE RESULTS

I. Interim results

In April, 28 answers were received. All regions were represented, with for 4 answers from Africa, 4 from Asia, 6 from the European region, 8 from the EEA (including the European Union), 3 from North America and 3 from South Asia.

An initial and preliminary analysis of the answers was conducted

The analysis was based on a factual synthesis of the responses received: only the answers "yes" or "no" indicated by the GPA member were taken into account, without analyzing the detailed answer provided.

It was decided to divide the answers into two categories: "yes" and "no and other", this latter category gathering:

- the "no" answers;
- the answers left unanswered;
- the answers left unanswered to the yes/no question but providing a detailed answer or comment;

At the end of the analysis, it appeared that:

(1) some "no" answers still needed to be confirmed in order to assess the observance or existence of the guarantee at stake;

(2) some responses left unanswered to the "yes/no" question but providing great details could be attributed to the "yes" category. For instance, one GPA member did not answer "yes" or "no" to the question on the statutory limitations, but indicated in the explanation that its legislation provided for a time limit during which the data can be processed by the government. Thus, it appears that statutory limitations do exist in this case and that this answer could be changed from "no and other" to "yes";

(3) a final and completed analysis should be drafted after having received late answers.

II. Final results

In July, 32 answers were received. 1 additional answer was received from an authority from Africa and 3 from the EEA (including the European Union).

Detailed answers regarding the main principles after an in-depth analysis and contacts with relevant GPA members.

GPA Global Privacy Assembly

CNIL.

Detailed answers

Are there guarantees and safeguards in your legal system to allow and frame government or public authorities' access to personal data held by the private sector for national and public security purposes?

	Yes	No or other provisions (TBC)
"Legal basis"	31	1
"Legislation clear and precise"	27	5
"Necessity and proportionality"	29	3
"Transparency to the individuals affected"	20	12
"Independent oversight mechanism"	27	5
"Statutory limitations of the data use"	30	2
"Redress and remedies"	30	2

Methodology

As before, the answers were divided into two categories: "yes" and "no and other".

Yes Category

This category includes the following answers:

"yes" answers given by the GPA member to the question with the corresponding explanation;	"yes" answers given by the GPA member while the corresponding explanation presents a principle and derogations (for instance, a GPA member indicated that the principle of individual notification is included in its legislation but it can be waived in specific situations);	"yes" answers given by the GPA member while the corresponding explanation indicates that the "yes" answer applies only to part of the question (for instance, some GPA members indicated that their national legislations provide for oversight mechanism but only ex post and not ex ante);	"no" answers when there appears to be an error or misinterpretation of the question by the responding GPA member and after having reached out to the GPA member (for instance, a GPA member answered "no" to the question "*Is there a requirement that the legislation has to be clear and precise with regard to government or public authorities' access (…)* ?" while a general requirement of clarity and accuracy of the law is provided for in the GPA member's national constitution);

« No and Other » Category

This category includes the following answers:

"no" answers ;	responses left unanswered (empty box);	Responses left unanswered to the "yes/no" question but providing important details on another related topic (for instance, to the question *"Is there a general principle of transparency to the individuals affected (notification)"* one GPA member did not answer "yes" or "no" but explained that, in the specific context of an investigation, the

		warrant authorizing the public authorities to have access to personal data must be communicated to the person who is the subject of the warrant, and/or to his or her counsel ; the GPA member added that a general obligation of publication should be provided for in legislation).

Final comments and caveat:

The following elements must be noted when interpreting the results, as they are not reflected in the results:

- The answers varied in details depending on the authority (responses ranged from 4 pages to 16 pages for the most detailed responses);

- Some authorities responded without being directly or fully designated as competent supervisory authority for the matters at stake;

- Out of 82 countries represented at the Global Privacy Assembly, we received 32 responses from GPA members: it represents a third of the membership. It must be pointed out that this sample still represent a significant portion of the membership and the geographical and legal/cultural is fairly represented.

- The principles put forward are not understood in the same way by all the authorities; some authorities have therefore replied specifying the differences of understanding and what their national standard is.

However, as the aim of the exercise is not to conduct a comparative analysis of actual legislations these caveats do not seem to invalidate the results. At the end, there did appear to be some common principles across different regions that could be advocated for by data protection authorities.

Indeed, as per the final results of the survey, it clearly appears that the principles reflected in the questionnaire are overall broadly observed or supported by GPA members, thus indicating commonalities in endorsing such principles when addressing guarantees in terms data protection and privacy applicable to government access to personal data.

III. Conclusions of the exercise

Initiating discussions and a dedicated activity in relation to guarantees against disproportionate government and public authorities' access to personal data has proven beneficial to the work of the Policy Strategy Working Group 1, both in terms of process and content wise. GPA members who have answered the questionnaire invested time in providing detailed feedback and express general support in pursuing the work on this matter.

Such exercise is also to be understood within the broader policy objective of placing the GPA as a key actor when it comes to international debates related to privacy and data protection. The discussion at international level on government access could benefit from the GPA input on this matter, which can now be substantiated by the result and analysis of this survey.

The survey results and analysis seem to indicate that the GPA, as an international community, could position itself on the international stage and advocate for the following data protection and privacy principles applicable to frame government access to data held by the private sector for the purposes of national security and public security:

Legal basis: it means that a legislation or binding principles in case law should frame government access;

A requirement that the legislation has to be clear and precise: this general principle is a requirement addressed to the legislator when drafting national laws on governments access. It appears from the answers to the questionnaire that the clarity and accuracy of the law regarding who can access the data, for what reasons, and for what data, were considered important elements by data protection authorities.

A general principle of necessity and proportionality of the access. Although this exact terminology is not used in all legislations, it appears to be an important principle to advocate for when data are accessed by governments; in addition, some GPA members have indicated that even though this principle was not explicitly provided for in their legislation, they wish to promote it as a general standard.

A general principle of transparency to the individuals affected. Even if derogations were mentioned regarding this principle and could be understood taken the nature of processing, it seemed to be generally agreed that a general principle of notification to the individuals is an important principle to advocate for.

An independent oversight mechanism. Even if different mechanisms of oversight were mentioned, a general consensus can be identified around a general oversight mechanism, ex ante (allowing the access) and ex post (once the data are accessed), is an important principle to advocate for.

Statutory limitations on the government's use of data after the data are acquired. This principle was largely shared by the GPA members and recognized as important.

Effective remedies and redress available to the individuals. This principle was largely shared by the GPA members and recognized as important.

The GPA, as an international community, can also advocate for the promotion of transparency reports by firms, identifying the number of requests received and their grounds. Even if this practice is not largely applicable or observed in GPA members jurisdictions, it appears important to highlight it as an important element to ensure trust, both from an individual/consumer and business point of view.

On this basis, the PSWG1 drafted an outline (see Appendix 2), highlighting those findings.

The GPA paper should be read as a recommendation from data protection authorities, expressing their willingness to see these principles and practice incorporated into international, regional and national legislations, for the benefit of individuals and companies in terms of data protection and privacy.

APPENDIX 1

QUESTIONNAIRE – ACCESS TO DATA BY GOVERNMENT AND PUBLIC AUTHORITIES FOR NATIONAL AND PUBLIC SECURITY PURPOSES

Background and mandate

The issue of disproportionate government and public authorities' access to personal data has become a relevant topic and is now on the agenda of different international fora (OECD, Council of Europe, United Nations and it also had been addressed at the G7 and G20 level).

In line with our commitment in Tirana and at the 2020 Closed Session to make the GPA a policy leader at the global level, the new Policy Strategy Working Group 1 ("PSWG 1") last year highlighted a need to identify key principles and common standards shared among data protection frameworks. At the end of the year, the adopted forward plan suggested that, in the context of that work, further consideration should be given to the issue of guarantees against disproportionate government and public authorities' access to personal data. This topic was specifically raised at the first meeting – year 2 of the PSWG1, to allow working group members to share their views on how it could be addressed. It was agreed that since Data Protection Authorities ("DPAs") are key stakeholders, the GPA should consider whether to issue a deliverable (nature to be determined) on this important topic to ensure that DPAs are part of the discussion.

Objectives

The idea would be to highlight the key principles we share and/or we can advocate for with regard to preventing disproportionate government or public authorities' access to personal data held by the private sector for national and public security purposes.

At the end, the PSWG1 could propose a deliverable (e.g. a high level statement), to be adopted at the next GPA closed session in Mexico 2021. In developing its proposal, PSWG1 would engage with selected other multilateral and intergovernmental fora already working on the issue.

As a first step, the working group implicated in this initiative has prepared a questionnaire to understand whether and which values and principles are shared on this topic among data protection authorities. You will find this questionnaire below. It will help us a lot if you can fill it out for your country.

Please complete and return to the PSWG 1 Secretariat via victoria.cetinkaya@ico.org.uk

QUESTIONNAIRE – GOVERNMENT OR PUBLIC AUTHORITIES'S ACCESS TO PERSONAL DATA HELD BY THE PRIVATE SECTOR FOR NATIONAL AND PUBLIC SECURITY PURPOSES

1° - Are there guarantees and safeguards in your legal system to allow and frame government or public authorities' access to personal data held by the private sector for national and public security purposes?	
Is there a legal basis (i.e. legislation or binding principles in case law) regarding government or public authorities' access to personal data held by the private sector for national and public security purposes?	Yes No Please specify
Is there a requirement that the legislation has to be clear and precise with regard to government or public authorities' access to personal data held by the private sector for national and public security purposes? For instance, clear information on the type of personal data accessed (e.g. Subscriber, traffic, content, etc.)	Yes No Please specify
Is there a specific requirement of necessity and proportionality for government to have access to the data?	Yes No Please specify
Is there a general principle of transparency to the individuals affected (notification[20]) regarding when and how the	Yes No Please specify

[20] Which could be subject to national limitations considering the specific nature of the activities

government can access personal data?	
Is there an independent oversight mechanism whose activities are governed by the rule of law to supervise access to personal data: - at the time of the collection of the personal data (e.g. government access required to be authorised by a special body)? - at the time the personal data is accessed by a public authority for further processing (e.g. oversight system provided for either by a judge or by another independent body)?	Yes No Please specify
Are there statutory limitations on the government's use of data after the data are lawfully acquired?	Yes No Please specify
Are there effective remedies and redress available to the individuals?	Yes No Please specify

2° - Which authority(ies) is(are) competent for the oversight of data processing in this field?

Are its independence and effectiveness ensured, if so, how?

3° - Has your country adopted any regulatory or policy measures mandating transparency reporting by firms in relation to government or public authorities' access to personal data held by the private sector for national and public security purposes?

Yes No Please specify

4° - Is there any other guarantee, safeguard in your legal system regarding government or public authorities' access to personal data held by the private sector for national and public security purposes?

Yes No Please specify

Thank you for your response. Please return the completed questionnaire to the PSWG1 Secretariat via victoria.cetinkaya@ico.org.uk

APPENDIX 2

Draft outline for a GPA Declaration/Statement on government access to data for national and public security purposes

Background/Recitals

Value of data protection and privacy principles for government access to data to promote trust and support international data flow.

Data protection and privacy principles applicable to government access to data are key elements ensuring respect for the rule of law and democratic values in relation to the legitmate objective of preserving national and public security.

GPA contribution to the ongoing discussion at international level, and in particular in light of the recent initiatives taken within various international fora (eg. OECD), to make data protection authorities' voice heard on such issue.

GPA data protection and privacy principles for government access to data

Scope : data protection and privacy principles applicable to the substantive and procedural conditions for government access to data held by the private sector for the purposes of national security and public security.

Principles :

- legal basis (i.e. legislation or binding principles in case law)
- requirement that the legislation has to be clear and precise (for instance, information about the type of personal data being accessed by the government must be clearly specified in a legislation)
- general principle of necessity and proportionality
- general principle of transparency to the individuals affected
- independent oversight mechanism (ex ante, i.e authorization to be required, and ex post, oversight mechanism when the data are accessed for further processing)
- statutory limitations on the government's use of data
- effective remedies and redress available to the individuals

Best practice:

- to promote transparency reporting by firms identifying the number of requests received and their grounds;

GPA call

Promote and implement the GPA data protection privacy principles for government access to data.

Government and international organisations to work towards the development of multilateral instrument ensuring adherence to key data protection and privacy principles in relation to government access to data.

Annex E: Draft resolution on government access to personal data

DRAFT RESOLUTION ON GOVERNMENT ACCESS TO DATA, PRIVACY AND THE RULE OF LAW: PRINCIPLES FOR GOVERNMENTAL ACCESS TO PERSONAL DATA FOR NATIONAL SECURITY AND PUBLIC SAFETY PURPOSES

Co-authors:

- Commission Nationale de l'Informatique et des Libertés (CNIL – France)
- Personal Information Protection Commission (PPC – Japan)
- Office of the Privacy Commissioner of Canada (OPC – Canada)

The 43nd Annual Closed Session of the Global Privacy Assembly

Having regard to the ICDPPC Resolution on the Conference's strategic direction (2019-21)[21]

Having regard to the ICDPPC Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights[22]

Having regard to the ICDPPC Resolution on transparency reporting[23]

RECALLING that respect for rule of law and democratic values lies at the core of data protection regimes and privacy laws,

CONSIDERING that protection and privacy principles applicable to government access to personal data and sensitive information are key elements ensuring respect for the rule of law and democratic values in relation to the legitimate objective of preserving national and public security,

RECOGNIZING that government authorities seeking access to personal data and sensitive personal information pursue and contribute to a legitimate public policy aim of preserving

[21] https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf

[22] https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf

[23] https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf

liberty and security, and that privacy safeguard help to augment the lawfulness, legitimacy and accountability of national security measures and public safety programs,

EMPHASIZING that strong data protections and privacy safeguards are vital for the preservation of citizen trust, the promotion of market interoperability and the support for international sharing of personal data and data flow,

NOTING that, in addition to the risks posed to privacy as a fundamental human right and to other fundamental right, the absence of sufficient privacy and data protection safeguards framing government access to data also raises serious challenges to the free flow of personal data at international level and may represent a hurdle to the global digital economy,

TAKING INTO ACCOUNT the important ongoing international initiatives and discussion at a range of fora (e.g. Council of Europe, OECD, G20/G7, United Nations) as well as bilateral negotiations and arrangements in relation to government access to personal data held by the private sector for national security and public safety purpose,

UNDERLINING the Global Privacy Assembly objective of enhancing its role and voice in wider digital policy debate at international level for the promotion of high standards and the need to ensure the mainstreaming of data protection and privacy in ongoing developments affecting the digital economy at international level,

The Global Privacy Assembly therefore adopts the following resolution on government access to data, privacy and the rule of law, advocating for the following principles to be applied for government access to personal data for national security and public safety purposes, thus laying down conditions ensuring that any type of public authorities legitimate access for purposes related to national security or public safety also contribute to the preservation of privacy and the rule of law:

1. **Legal basis**: Government access to personal data must be duly authorized by appropriately enacted legislation, after public debate and scrutiny by legislators.

2. **Clear and precise legislation applying to government access**: any legislation authorizing access to personal information should be:

   a) publicly available,

   b) written in clear, easily understandable language, and,

   c) precise and specific as to the scope of personal information for which the law is granting governmental access and the conditions for such access.

3. **General principle of necessity and proportionality**: in order for data access by state authorities to be justifiable, the specific usage for personal information must be linked to a demonstrably necessary function or activity of government, and that the intrusiveness must be proportionate to the goal in question.

4. **Transparency to the individuals affected:** Any agreement or arrangement for government access, flowing from authorization in law, should also make proactive, baseline public reporting a requirement for government agencies involved.

5. **Independent oversight:** laws authorizing access should ideally provide for both independent advance oversight (e.g. prior judicial authorization) as well as retrospective review (e.g. auditing of processing by independent regulatory body).

6. **Statutory limitation on government's use of data acquired:** law authorizing government access to personal data for one specific purpose should regulate and frame any secondary use or onward transfer for other purposes.

7. **Effective remedies and redress available to the individuals affected**: any agreement or arrangement for governmental access to data, flowing from authorization in law, should include specific provisions for any individuals affected to seek judicial redress and tangible remedies.

Complementary to the principles above, **the Global Privacy Assembly considers the following examples and best practices as relevant illustrations of further accountability in government access to personal data and concretisations of key safeguards** ensuring the protection of privacy and personal data of individuals:

- **Transparency reporting** by commercial firms documenting numbers of government requests;
- **Additional avenues** for private sector and individuals remedy and redress in relation to government access to personal data;
- **International regulatory cooperation** for oversight and supervision of government access to personal data.

The Global Privacy Assembly resolves to promote and advocate for the above-mentioned principles and best practices for governmental access to personal data for national security and public safety purposes.

The Global Privacy Assembly hereby calls on governments and international organisations to observe the above-mentioned principles and to work towards the development of multilateral instruments ensuring adherence to key data protection and privacy principles in relation to government access to personal data.

Annex F: Report, analysis and initial list of key data protection terms and their meanings

Data protection terms and their meanings

Summary of analysis and report

1. Introduction

At the 41st Conference of the Global Privacy Assembly (GPA) in 2019, a Resolution on the Conference's Strategic Direction was adopted. This set out the GPA's Strategic Plan for 2019-21, and included a Policy Strategy to aid its implementation.

To implement the first strategic priority to 'Work towards a global regulatory environment with clear and consistently high standards of data protection,' the Policy Strategy committed the GPA to delivering several actions. Two of those actions related to global frameworks and standards, as follows:

Action 1: Complete an analysis of current frameworks for privacy and data protection, including key principles, data subject rights, cross border transfers and demonstrable accountability standards. This action was delivered in 2020, with the adoption of the Policy Strategy Workstream 1: Global Frameworks and Standards Working Group's analysis of ten global data protection and privacy frameworks at the 42nd GPA Conference.

Action 2: Consider developing common definitions of key data protection terms.

Terms and their meanings are vitally important. The work of the GPA on global frameworks and standards in 2019-21 has focused on identifying commonality in global and regional privacy and data protection frameworks and instruments. It's therefore important to understand what is meant by the key terms in those frameworks and instruments, and to identify where shared meanings exist across frameworks.

This piece of work will be a rolling project that will continue beyond 2021. The project's work in 2021 started with identifying a list of terms where definitions already exist in the frameworks. Those terms were analysed to identify any commonality, and then we have attempted to develop shared definitions that can be agreed on across the GPA, and across those who use the frameworks. It should be noted that the definitions that will be developed as part of this work will not be legal definitions. Instead we will use the existing definitions to develop practical meanings of the terms.

2. Identifying the terms to define

In order to decide on a list of terms to define, the ten global frameworks from the 2020 analysis were analysed again, this time to extract the already-defined terms in each of the frameworks. 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
- African Union Convention on Cyber Security and Personal Data Protection
- ECOWAS Supplementary Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

Terms that had definitions in each framework were extracted and the definitions noted. The extracted terms can be found in the table in annex 1.

Most of the frameworks analysed include several defined terms. However, the initial analysis found that there were relatively few formally defined terms in the frameworks. For this reason, the list of terms was broadened, and terms that were less formally defined were added to the list in Appendix 1. The list of terms in Appendix 1 therefore includes both formally defined terms, such as 'personal data' and terms whose meaning is indirectly set out in the frameworks, perhaps by reference to the essential elements of a concept, such as 'accountability,' in order to obtain a broader range of terms for consideration.

The list of extracted terms includes:

- Personal data (formally defined in nine of the ten frameworks)
- Processing (formally defined in seven frameworks, with the meaning indirectly implied in one)
- Data subject ((formally defined in eight frameworks)
- Controller (formally defined in nine frameworks)
- Processor (formally defined in eight frameworks)
- Third party (formally defined in three frameworks)
- Recipient (formally defined in four frameworks)
- Supervisory authority (formally defined in four frameworks, with the meaning indirectly implied in five)
- Sensitive data (formally defined in seven frameworks)
- Profiling (formally defined in two frameworks)

- Anonymisation (formally defined in one framework, with the meaning indirectly implied in two)
- Pseudonymisation (formally defined in one framework, with the meaning indirectly implied in two)
- Consent (formally defined in four frameworks, with the meaning indirectly implied in two)
- Personal data breach (formally defined in two frameworks, with the meaning indirectly implied in two)
- Transborder flows of personal data (formally defined in one framework, with the meaning indirectly implied in two)
- Accountability (not formally defined in any framework but meaning indirectly implied in six)
- Transparency (not formally defined in any framework but meaning indirectly implied in seven)
- Data protection / privacy by design and default (not formally defined in any framework but meaning indirectly implied in five)
- Data protection / privacy impact assessment (not formally defined in any framework but meaning indirectly implied in four)
- Privacy management programme (not formally defined in any framework but meaning indirectly implied in two)
- Binding corporate rules (not formally defined in any framework but meaning indirectly implied in two)

By including terms that also had their meaning indirectly implied in the frameworks, the list was able to be expanded. It can be noted that although the list above does include some core terms that would be helpful to define, such as terms about the nature of the data, and about actors and actions in the processing of personal data, terms relating to core principles (such as fairness, proportionality or data minimisation) are not included. As the work in 2021 is focusing on terms that have some degree of existing definition in the frameworks, and these do not, terms relating to core principles are therefore not included in this year's work, but will be considered as a priority in the next list of definitions for 2022.

3. Analysis of commonality and difference

Once the definitions and meanings had been extracted from the frameworks, they were analysed and compared. The analysis results can be seen in the table in Annex 2. Several of the terms had substantial commonality in their definitions and meanings across the frameworks – this could be seen with the terms 'personal data'; 'processing'; 'data subject';

‘controller’; ‘processor’; ‘third party’; ‘sensitive data’; ‘consent’; ‘personal data breach’; ‘privacy management programme’ and ‘binding corporate rules’.

It should, however, be noted that even where there is substantial commonality, this does not mean that a term’s meaning is identical across the frameworks. While the formal definition may be the same, some terms had lists of examples, or further descriptions, that were different to others with the same core definition. The definitions / meanings that this work develops will not be able to include all such differences, and instead will attempt to find relatively high-level and more general meanings in order to highlight commonality and areas of agreement.

In addition, there are some terms for which there is commonality in meaning, but only a small number of frameworks define them. These terms include ‘third party’; ‘profiling’; ‘anonymisation’; ‘pseudonymisation’; ‘personal data breach’; ‘privacy management programme’; and ‘binding corporate rules’. No substantial differences in definition were found for these terms, however, and the lack of definition in some frameworks could mean either that a term is not routinely used within that framework, or that it is but that no need was identified to formally define it. While the smaller number of common definitions may somewhat reduce the strength of the argument to include these terms, in the absence of substantial differences in definitions they have been included in our list of defined terms.

Regarding differences between the definitions, while there were some differences found across several terms and frameworks, these were mostly able to be dealt with by including a simplified definition in our list. One term proved difficult to develop a simplified definition: the term ‘transborder flows of personal data’ was only defined by three frameworks but where two frameworks defined the term as the movement of personal data across borders, a third defined it as the disclosure or making available to a recipient subject to another jurisdiction or international organisation. The difference between these two meanings means that developing a high level, accurate and simple meaning, that is compatible with both, will require further work. This term has therefore not been included in the final list and instead will be considered in 2021-22. The term ‘BCRs’ is also therefore not included in this year’s list, because it would be preferable to keep terms relating to international transfers together. Only one term showed significant differences: the term ‘recipient’ is described in several different ways by different frameworks – as the person to whom data are disclosed, the person to whom data may be disclosed, and the person entitled to receive personal data. For this reason, this term will also not be included in our list of defined terms. The remaining 18 terms will be included.

4. Conclusion: the GPA’s list of privacy and data protection terms, and their meanings – and next steps

The analysis of defined terms in the frameworks as described above, and as shown in Appendices 1 and 2, has concluded in 2021 with the production of an initial list of 18 privacy and data protection terms and their meanings. The list can be found in Appendix 3.

The meanings have been developed from those found in the frameworks. In most cases they are not identical with the framework definitions but instead aim to be consistent, or at least not to contradict, any of them.

The terms have been grouped into categories of like terms: terms relating to the data; to the actors involved in its processing; to the actions carried out in relation to the data; key concepts; measures; and supervision and enforcement. As the project develops in 2021-22 and beyond, other categories of terms will be added, with the next step to address definitions relating to core principles.

Appendix 1: Comparison table: data protection terms defined in the 10 frameworks analysed in 2019-20 by GPA Policy Strategy Working Group 1: Global frameworks and standards, and their definitions

Note: An initial analysis of the ten frameworks found that there were relatively few formal definitions provided in the frameworks. For this reason, we have added to the table terms that are less formally defined, and terms whose meaning is indirectly set out, for example by reference to the essential elements of a concept, in order to obtain a broader range of terms for consideration.

	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
Definitions										
Personal data	**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**		**Definition:**

	‘Personal data’ – any information relating to an identified natural person or a person who may be identified by means reasonably likely to be used.	‘Personal data’ - any information relating to an identified or identifiable individual (data subject).	‘Personal information’ – any information about an identified or identifiable individual.	‘Personal data’ – any information relating to an identified or identifiable individual (‘data subject’). **The protection of individuals with regard to automatic processing of personal data in the context of**	‘Personal data’ – any information relating to an identified or identifiable individual.	‘Personal data’ - any information regarding an individual identified or identifiable, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, acoustic way, or of any other kind. It is considered that a person is	‘Personal data’ – any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more	‘Personal data’ - any information relating to an identified or identifiable natural person (‘data subject’).		‘Personal data’ – any information relating to an identified individual or who may be directly or indirectly identifiable by reference to an identification number or one of several elements related to their physical, physiological, genetic, psychological, cultural, social or

				profiling Recommendation CM/Rec (2010) 13 and explanatory memorandum adds: 'An individual is not considered 'identifiable' if identification requires unreasonable time or effort.'		identifiable when his identity can be determined directly or indirectly, provided that this does not require disproportionate deadlines or activities.'	factors specific to his/her physical, physiological, mental, economic, cultural or social identity.			economic identity.

Processing	**Definition:** 'Processing' – any operation or set of operations, automated or not, which is performed on personal data, such as collection, storage, use, disclosure or deletion.		**Meaning provided indirectly:** Meaning of 'use' is informally set out as follows, which includes 'processing' as a less broad activity: 'Unless the context suggests otherwise, 'use' of personal information	**Definition:** 'Automatic processing' – includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration,	**Definition:** 'Data processing' – any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the	**Definition:** 'Treatment' – any operation or set of operations performed through physical or automated procedures on personal data (includes collection, access, registration, organisation, structuring, adaptation, indexation, modificatio	**Definition:** 'Processing of personal data' – any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as the collection, recording, organization, storage, adaptation, alteration,	**Definition:** 'Processing' - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,		**Definition:** 'Personal data processing' – any operation or set of operations carried out or not, with the assistance of processes that may or may not be automated, and applied to data, such as obtaining, using, recording, organisation, preservation, adaptation, alteration, retrieval,

			should be considered to include collection, holding, processing, use, disclosure or transfer of personal information.'	erasure, retrieval or dissemination. **Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the**	carrying out of logical and / or arithmetical operations on such data	n, extraction, consultation, storage, preservation, development, transfer, dissemination, possession, exploitation – in general any use or disposal	retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data.	storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction		saving, copying, consultation, utilisation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, encryption, erasure or destruction of personal data.

				context of profiling: 'Processing' means any operation or set of operations carried out partly or completely with the help of automated processes and applied to personal data, such as storage, conservation, adaptation or						

				alteration, extraction, consultation, utilisation, communication, matching or interconnection, as well as erasure or destruction. '						
Data subject	**Definition:** 'Data subject' – the natural person whose	**Definition:** 'Data subject' – the identified or identifiable individual		**Definition:** 'Data subject' – the identified or identifiable individual	**Definition:** 'Data subject' – the identified or identifiable individual	**Definition:** 'Holder' – individual to whom the personal	**Definition:** 'Data subject' – any natural person that is the subject of	**Definition:** 'Data subject' – an identified or identifiable person [to		**Definition:** 'Data subject' – an individual who is the subject of

	personal data are subject to processing.	[to whom the] personal data relates.		[to whom the] personal data relates.	[to whom the] personal data relates.	data concern	personal data processing	whom the] personal data relates.		personal data processing.
Controller	**Definition:** 'Responsible person' – means any natural person or organization, public or private which, alone or jointly with others, decides on	**Definition:** 'Data controller'- a party who, according to national law, is competent to decide about the contents and use of personal data regardless	**Definition:** 'Personal information controller' – person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information	**Definition:** 'Controller of the file' – the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide	**Definition:** 'Controller' – the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-	**Definition:** 'Person responsible' – individual or legal private entity, public authority, services or body that, alone or together with others, determines the	**Definition:** 'Data controller' – any natural or legal person, public or private, any other organization or association which alone or jointly with others, decides to	**Definition:** 'Controller' - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the		**Definition:** 'Data controller' means any public or private individual or legal entity, body or association who, alone or jointly with others, decides to collect and process

	the processing .	of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.	. It includes a person or organization who instructs another person or organization to collect, hold, use, process, use, transfer, disclose personal information on his or her behalf, but excludes a person or organization who performs such	what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them. **Recommendation CM/Rec(2010)13 of the Committee of Ministers**	making power with respect to data processing	purposes, means, scope and other matters related to the treatment of personal data	collect and process personal data and determines the purposes.	purposes and means of the processing of personal data		personal data and determines the purposes for which such data are processed.

			functions as instructed by another person or organizatio n. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.	**to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling** adds**:** 'Controller' means the natural or legal person, public						

				authority, agency or any other body which alone, or in collaboration with others, determines the purposes of and means used in the collection and processing of personal data.						
Processor	**Definition:**		**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**	**Definition:**		**Definition:**

	'Processing service provider' – means any natural person or organization, other than the responsible person that carries out processing of personal data on behalf of such responsible person.		'Personal information processor' – no formal definition, but reference is made to a personal information processor providing effective implement-ation of a personal information controller's privacy obligations related to the processing	**Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling:**	'Processor' – a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller	'Person in charge' – a service provider (individual, legal entity or public authority) that treats personal data on behalf of the person responsible	'Sub-contractor' – any natural or legal person, public or private, any other organization or association that processes personal data on behalf of the data controller.	'Processor' - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller		'Data processor' – any public or private individual or legal entity, body or association who processes personal data on behalf of the data controller.

			of personal information .	'Processor' means the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.						
Third party							**Definition:** 'Third party' – a natural or legal person, public	**Definition:** 'Third party' - a natural or legal person, public		**Definition:** 'Third party' – any public or private individual or legal entity,

							authority, agency or body, other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor are authorized to process the data.	authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data		body or association other than the data subject, the data controller, the data processor and any other persons placed under the direct authority of the data controller or the data processor, who is authorised to process data.
Recipient					**Definition:**		**Definition:**	**Definition:**		**Definition:**

					'Recipient' – a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available.		'Recipient of processed personal data' – any person entitled to receive communication of such data other than the data subject, the data controller, the sub-contractor and persons who, for reasons of their functions,	'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Does not include public authorities which may receive personal		'The recipient of personal data processing' – any individual to whom the data may be disclosed, and who is not the data subject, the data controller, the data processor, or persons who by virtue of their functions are responsible for processing such data.

							have the responsibility to process the data.	data in the framework of a particular inquiry in accordance with Union or Member State law		
Supervisory Authority	**Meaning provided indirectly:** Described as 'supervisory authorities' […] 'that will be responsible for supervisin	**Definition:** 'Privacy enforcement authority' - any public body, as determined by each Member country, that is responsible for	**Definition:** 'Privacy Enforcement Authority' – any public body responsible for enforcing privacy laws and that has powers to conduct	**Meaning provided indirectly:** **Additional Protocol to the Convention for the Protection of Individuals with regard to**	**Meaning provided indirectly:** Each Party shall provide for one or more authorities to be responsible for ensuring compliance	**Meaning provided indirectly:** 'Control / Supervision Authority' - 'There must be one or more control authorities on personal data	**Meaning provided indirectly:** 'National Personal Data Protection Authority' – 'Each State Party shall establish an	**Definition:** 'Supervisory authority - an independent public authority which is established by a Member State		**Definition:** 'Authority of Protection' – the data protection authority shall be an independent administrative authority responsible for ensuring that personal

	g the observance of the principles set out in this Document.'	enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings. **Further meaning provided in the Supplementary explanatory memorandum to the**	investigations and/or pursue enforcement proceedings.	**Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows:** 'Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic	with the provisions of this Convention.	protection in each Ibero-American State, with full autonomy, in accordance with their applicable national legislation. Control authorities may be single-member or multiple-member bodies; they shall act impartially and independen	authority in charge of protecting personal data. The national protection authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions	pursuant to Article 51		data is processed in compliance with the provisions of this Supplementary Act.

		revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013): '..a "privacy enforcement authority" refers not only to those public sector		law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.'		tly in their jurisdictions, and they shall be free or any external influence, whether direct or indirect, and they shall not request nor admit any order or instruction.'	of this Convention. '			

		entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they have the powers to conduct investigations or bring proceedings								

		in the context of enforcing "laws protecting privacy".								
Sensitive data	**Definition:** The following personal data shall be deemed to be sensitive: a. Data which affect the data subject's			**Definition:** 'Special categories of data' – Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal	**Definition:** 'Special categories of data' – '..genetic data; personal data relating to offences, criminal proceedings and convictions, and related	**Definition:** 'Sensitive Personal Data' - those that refer to the intimate sphere of their holder, or which undue use may originate discriminati	**Definition:** 'Sensitive data' – all personal data relating to religious, philosophic al, political and trade-union opinions and activities, as well as to	**Definition:** 'Special categories of personal data' – 'personal data revealing racial or ethnic origin, political opinions, religious or philosophic		**Definition:** 'Sensitive data' – personal data relating to an individual's religious, philosophical, political, trade union opinions or activities, to his sexual life, racial origin or health,

	most intimate sphere; or b. Data likely to give rise, in case of misuse, to: i. Unlawful or arbitrary discrimination; or ii A serious risk to the data subject.. 2. In particular, those personal data			data concerning health or sexual life […] personal data relating to criminal convictions. **The protection of individuals with regard to automatic processing of personal data in the context of profiling Recommen**	security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life..'	on or involve a serious risk thereto. In an illustrative way, personal data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; union affiliation; political opinions;	sex life or race, health, social measures, legal proceedings and penal or administrative sanctions.	al beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual		relating to social measures, proceedings, and criminal or administrative sanctions.

	which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive			**dation CM/Rec (2010) 13 and explanatory memorandum** 'Sensitive data' – personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex		information regarding health, life, sexual preference or orientations, genetic data or biometric data aimed at identifying the person in an unequivocal way.'		orientation. '		

	data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.			life or criminal convictions, as well as other data defined as sensitive by domestic law.'						
Profiling					**Definition:** **Recommendation**			**Definition:** 'Profiling' - any form of		

					CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling: "Profile" refers to a set of data characterisi			automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performanc e at work, economic		

					ng a category of individuals that is intended to be applied to an individual. "Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take			situation, health, personal preferences, interests, reliability, behaviour, location or movements.		

					decisions concerning her or him or for analysing or predicting her or his personal preferences , behaviours and attitudes. (NB not legally binding) .					
Anonymisation					**Meaning provided indirectly:** **Paragraphs 18-20 of the Explanatory**	**Definition:** 'Anonymization: the application of measures of any kind aimed at preventing		**Meaning provided indirectly:** 'anonymous information , namely information		

					Report refer to 'anonymous' data: 'The use of a pseudonym or of any digital identifier / digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised.' ' Data is to be	the identification or re - identification of an individual without disproportionate efforts.'		which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. '		

					considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, taking into consideration the available technology at the time of the					

					processing and technological developments.'					
Pseudonym-isation					**Meaning provided indirectly:** **Article 18 of the Explanatory Report** refers to 'pseudonymous' data: ' The use of a pseudonym or of any digital identifier/	**Meaning provided indirectly:** **Article 2.1.a** defines anonymization broadly, as 'the application of measures of any kind aimed at preventing the identification or re -		**Definition:** 'Pseudonymisation' - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the		

					digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the	identification of an individual without disproportionate efforts.		use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable		

					Convention. ’			natural person;		
Consent	**Meaning provided indirectly:** ‘..personal data may only be processed after obtaining the free, unambiguous and informed consent of the data subject.’ ‘The responsibl				**Meaning provided indirectly:** **Article 5.2** ‘Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent	**Definition:** ‘Consent: expression of the free, specific, unequivocal and informed will of holder through which he accepts and authorizes the treatment of the personal data that	**Definition:** ‘Consent of data subject’ – any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty	**Definition:** ‘Consent’ of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear		**Definition:** ‘Consent of the data subject’ – any manifestation of specific, unequivocal, free, informed and express will by which the data subject or his legal, judicial or agreed representative accepts that his personal data be

	e person shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the				of the data subject or of some other legitimate basis laid down by law.' **Explanatory report paragraph 42** The data subject's consent must be freely given, specific, informed and unambiguous. Such consent	concern him.'	representative accepts that his/her personal data be subjected to manual or electronic processing.	affirmative action, signifies agreement to the processing of personal data relating to him or her.		processed either manually or electronically.

	responsible person.’				must represent the free expression of an intentional choice, given either by a statement (which can be written, including by electronic means, or oral) or by a clear affirmative action and which clearly indicates in this specific context the acceptance					

					of the proposed processing of personal data.					
Personal Data Breach		**Meaning provided indirectly:** The Security Safeguards Principle says that 'Personal data should be protected by reasonable security safeguards against such			**Meaning provided indirectly:** '..accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.'	**Definition:** 'a violation to the safety of personal data.. ..understood as any damage, loss, alteration, destruction, access and, in general, any illegal or non - authorized		**Definition:** 'Personal data breach' - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,		

		risks as loss or unauthorised access, destruction, use, modification or disclosure of data.' The risks are described in the Supplementary Explanatory Memorandum in the context of 'data breaches' and				use of personal data, even if it occurs accidentally.'		personal data transmitted, stored or otherwise processed.		

		'security breaches'.								
Transborder flows of personal data		**Definition:** 'Transborder flows of personal data' – movements of personal data across borders.		**Meaning provided indirectly:** 'Transborder flows of personal data' are described as 'the transfer across national borders, by whatever medium, of personal data undergoing automatic	**Meaning provided indirectly:** **Explanatory Report paragraph 102**: '…A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to					

				processing or collected with a view to their being automatically processed.	the jurisdiction of another State or international organisation'					
Accountability	**Meaning provided indirectly:** The responsible person shall: a. Take all the necessary measures to observe the	**Meaning provided indirectly:** 'A data controller should be accountable for complying with measures which give effect to	**Meaning provided indirectly:** 'A personal information controller should be accountable for complying with measures that give		**Meaning provided indirectly (although term itself is not used, the concept is included unnamed in the framework, under 'Additional obligations'):**	**Meaning provided indirectly:** 'The person responsible shall implement the necessary mechanisms to prove compliance with the principles		**Meaning provided indirectly:** 'The controller shall be responsible for, and be able to demonstrate compliance with [the data		

	principles and obligations set out in this Document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both	the principles.' A data controller should: a) Have in place a privacy management programme that: i. gives effect to these Guidelines for all personal data under its control; ii. is tailored to the structure, scale,	effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller		'Each Party shall provide that controllers 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	and obligations established in these Standards, and shall also be accountable to holder and to the control authority for the treatment of personal data in its possession, for which it may use standards, best national or international practices, self-		protection principles].		

	to data subjects and to the supervisory authorities in the exercise of their powers.	volume and sensitivity of its operations; iii. provides for appropriate safeguards based on privacy risk assessment; iv. is integrated into its governance structure and establishes internal oversight mechanisms; v. includes plans for responding	should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently		compliance with the provisions of this Convention. ’	regulation schemes, certification systems, or any other mechanism it deems appropriate for such purposes.’				

		to inquiries and incidents; vi. is updated in light of ongoing monitoring and periodic assessment; b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent	with these Principles.' 'A useful means for a personal information controller to help ensure accountability for the personal information it holds is to have in place a privacy management programme.'							

		privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and c) Provide notice, as appropriate, to privacy enforcement authorities								

		or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected								

		data subjects.								
Transparency	**Meaning provided indirectly:** 'Openness' - Every responsible person shall have transparent policies with regard to the processing of personal data.	**Meaning provided indirectly:** 'Openness' - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means	**Meaning provided indirectly:** 'Notice' – Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to		**Meaning provided indirectly:** 'Transparency' – 1. Each Party shall provide that the controller informs the data subjects of: a. his or her identity and habitual residence or	**Meaning provided indirectly:** 'Transparency' - 16.1. The person responsible shall inform holder about the existence and main characteristics of the treatment to which its personal data shall be		**Meaning provided indirectly:** 'Transparency' - Any processing of personal data should be […] transparent to natural persons that personal data concerning them are collected, used,		**Meaning provided indirectly:** 'The principle of transparency implies that the data controller is obliged to provide information about the processing of personal data.'

	2. The responsible person shall provide to the data subjects, as a minimum, information about the responsible person's identity, the intended purpose of processing, the recipients to whom their personal data will	should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information		establishment; b. the legal basis and the purposes of the intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal	submitted, in order to make informed decisions on this regard. 16.2. The person responsible shall provide holder, at least the following information: a. Its identity and contact information.		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 communication relating to the processing of those personal data be easily		

	be disclosed and how data subjects may exercise the rights provided in this Document, as well as any further information necessary to guarantee fair processing of such personal data.		might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and		data, if any; and e. the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.	b. The purposes of the treatment to which its personal data shall be submitted. c. The communications, whether national or international, of personal data that it intends to perform, including the recipients and the		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 purposes of the processing and further information to ensure fair and		

	3. When personal data have been collected directly from the data subject, the information must be provided at the time of collection, unless it has already been provided. 4. When personal data have		means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information. This Principle is directed towards ensuring that			purposes that give rise to the performance thereof. d. The existence, form and mechanisms or procedures through which it may exercise the access, correction, cancellation, opposition and portability rights. e. If applicable,		transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of		

	not been collected directly from the data subject, the responsible person must also inform him/her about the source of personal data. This information must be given within a reasonable period of time, but may be replaced		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 controllers may enable an individual to make a more informed decision about interacting			the origin of the personal data when the person responsible did not obtain them directly from holder. 16.3. The information provided to holder must be sufficient and easily accessible, as well as written and structured in a clear		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 for which personal data are processed should be explicit and legitimate		

	by alternative measures if compliance is impossible or would involve a disproportionate effort by the responsible person. 5. Any information to be furnished to the data subject must be provided		with the organization.			and simple language, easy for holders to whom it is addressed to understand, especially in the case of girls, boys and adolescents. 16.4. Every person responsible shall have transparent policies for the treatment of the personal		and determined at the time of the collection of the personal data. The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand,		

	in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors. 6. Where personal data are collected on line by means of electronic communications networks,					data that it performs.		and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of		

	the obligations set out in the first and second paragraphs of this section may be satisfied by posting privacy policies that are easy to access and identify and include all the information							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		

	mentioned above.							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.		
Data protection / privacy by design and default	**Some meaning provided indirectly:** The adaptation of information systems and/or technologies for the processing of personal data to the	**Meaning provided indirectly:** **Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy**			**Meaning provided indirectly:** 'Each Party shall provide that controllers, and, where applicable, processors, examine the likely impact of intended data processing on the rights and	**Meaning provided indirectly:** 'Privacy due to design and Privacy by default' - 'The person responsible shall apply, from the design, in the determination of the treatment means of personal		**Meaning provided indirectly:** 'Data protection by design and by default' – 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and		

	applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the developm	**and transborder flows of personal data (2013):** 'Privacy by design', whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an			fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.'	data, during and before the collection of personal data, preventive measures of various natures that allow effectively applying the principles, rights and other obligations provided in the applicable national legislation of the Ibero-		purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the		

	ent and implement ation thereof.	afterthough t.				American State. The person responsible shall guarantee that its programs, services, computing systems or platforms, electronic applications or any other technology that implies a treatment of personal data, comply by default or adapt to		time of the processing itself, implement appropriate technical and organisatio nal measures, such as pseudonymi sation, which are designed to implement data-protection principles, such as data minimisatio n, in an effective manner and		

						the principles, rights and other obligations provided in the applicable national legislation of the Ibero-American State. Specifically, with the purpose that only a minimum of personal data is subject to treatment, and that the		to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures		

						accessibility thereof is limited, without holder's interventio n, to an undetermin ed number of persons.		for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing,		

								the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.		

Data protection / privacy impact assessment		**Meaning provided indirectly:** **Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of**			**Meaning provided indirectly:** 'Each Party shall provide that controllers, and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data	**Some meaning provided indirectly:** 'Impact assessment on the protection of personal data' - 'When the person responsible intends to perform a type of treatment of personal data that due to its nature,		**Meaning provided indirectly:** 'Data protection impact assessment' - 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the		

		personal data (2013): 'Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy. This process			subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.'	context or purposes probably entails a high risk of affecting the right to the protection of holders' personal data, it shall perform, prior to the implementation thereof, an impact assessment on the protection of personal data.'		processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection		

		is sometimes accomplished by conducting a “privacy impact assessment ” before a new programme or service is introduced or where the context of the data use changes significantly .						of personal data. […] ‘ The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by		

								the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph		

								1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and		

								legitimate interests of data subjects and other persons concerned.'		
Privacy management programme		**Some meaning provided indirectly:** **In OECD Guidelines Part Three, and supplementary explanatory memorandum:** Privacy management	**Some meaning provided indirectly:** An operative privacy management programme will provide a sound basis for a personal information							

		programmes: These serve as the core operational mechanism through which organisations implement privacy protection. A data controller should: a) Have in place a privacy management programme that: i. gives effect to these Guidelines for all personal data under its control;	controller to demonstrate that it is complying with measures that give effect to the privacy protections in the Framework. Accordingly, member economies should consider encouraging personal information controllers to develop							

		ii. is tailored to the structure, scale, volume and sensitivity of its operations; iii. provides for appropriate safeguards based on privacy risk assessment; iv. is integrated into its governance structure and establishes internal oversight mechanisms; v. includes plans for	and implement privacy management programmes for all personal information under their control. Privacy management programmes should: a) be tailored to the structure and scale of the operations of the							

		responding to inquiries and incidents; vi. is updated in light of ongoing monitoring and periodic assessment;	personal information controller, as well as the volume and sensitivity of the personal information under its control; b) provide appropriate safeguards based upon risk assessment that takes into account the potential harm to individuals;							

			c) establish mechanisms for internal oversight and response to inquiries and incidents; d) be overseen by designated accountable and appropriately trained personnel; and e) be monitored and be							

			regularly updated.							
Binding corporate rules	**Meaning provided indirectly:** [Where] a transfer [is] carried out within corporations or multinational groups, guarantees may be contained in internal privacy rules, complianc							**Meaning provided indirectly:** An appropriate safeguard to enable the transfer of personal data to a third country. Approved, legally binding rules that apply to and are enforced by		

	e with which is mandatory.							every member concerned of [a] group of undertaking, or group of enterprises engaged in a joint economic activity, including their employees, and that expressly confer enforceable rights on data subjects with regard to the		

								processing of their personal data.		

Appendix 2: Terms defined (or meaning provided indirectly in the framework text, explanatory notes or equivalent)

(**Please note**: numbers in brackets refer to the number of frameworks particular wording appears in.)

Defined terms	Frameworks defined in	Comments: Commonalities in meaning	Comments: Significant differences in meaning	Dictionary definition, where relevant
Personal data	9 – all bar UN Guidelines	**Substantial commonality.** **Term used:**	**No significant difference** in the definitions as written in the framework texts.	

		Personal data (8) /personal information (1) **Meaning:** Information relating to (7) / about (1) / regarding (1) an identified or identifiable individual (6) / natural person (3).	• However, it is important to note that some frameworks include further text on the meaning of 'identifiable', which highlights more differences in practice.	
Processing	8 – all bar OECD and UN Guidelines	**Substantial commonality.** **Term used:** Processing (6) / use (1) / treatment (1) **Meaning:** Any operation or set of operations (7) performed on personal data, such as collection (6), obtaining (1), recording (3), saving (1), copying (1), storage (6),	**Some difference.** • Most frameworks use the term 'processing'. APEC uses the term 'use', with the term 'processing' as a less broad activity within that.	To arrange (documents etc) systematically, to examine and analyse, to perform operations on data, to subject data to such operations.

		holding (1), use (5), utilisation (2), disclosure (6), making available (4), access (1), deletion (1), erasure (5), destruction (5), transfer (2), communication, (1), alteration (5), retrieval (5), dissemination (5), conservation (1), preservation (3), adaptation (5), extraction (2), consultation (5), matching (1), registration (1), organisation (4), structuring (2), indexation (1), modification (1), development (1), possession (1), exploitation (1), disposal (1), backup (1), copying (2), alignment or combination (3), encryption (2), blocking (1), restriction (1)		
Data subject	8 – all bar APEC Privacy Framework and UN Guidelines	**Substantial commonality.** **Term used:** Data subject (7) / holder (1)	**No significant difference** in the definitions as written in the framework texts.	

		Meaning: The identified or identifiable (4) individual (5) / natural (2) person (3) to whom the personal data relates (4) / concern (1) / whose personal data are subject to processing (1) / that/who is the subject of personal data processing (2)		
Controller	9 – all bar UN Guidelines	**Substantial commonality.** **Term used:** Responsible person (1) / Data controller (3) / Personal information controller (1) / Controller of the file (1) / Controller (2) Person responsible (1) **Meaning:**	**No significant difference** in the definitions as written in the framework texts.	

		Any natural or legal person, public or private body (6) / person or organization (1) / party who is competent according to national law (2) and who, alone or jointly/in collaboration/together with others (7) decides (6) / determines (2) / controls (1) the purpose of processing (5) / collection (3) / use/processing (4) / means of processing (2) the personal data.		
Processor	8 – all bar OECD and UN Guidelines	**Substantial commonality.** **Term used:** Processor (3) / Data processor (1) / Personal information processor (1) Processing service provider (1) / Person in charge (1) / Sub-contractor (1)	**No significant difference** in the definitions as written in the framework texts.	

		Meaning: Any natural or legal person, public or private body (6) / service provider (1) / that processes/treats personal data on behalf of the controller/person responsible (7)		
Third party	3 – African Union Convention; GDPR; ECOWAS	**Significant commonality.** **Term used:** Third party (3) **Meaning:** A natural or legal person (2) / individual or legal entity (1), public authority or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or	**No significant difference** in the definitions as written in the framework texts – although only three frameworks define the term.	

		processor, are authorised to process the personal data (3).		
Recipient	4 – C108+; African Union Convention; GDPR; ECOWAS	**Some commonality.** **Term used:** Recipient (2) / recipient of processed personal data (1) / recipient of personal data processing (1) **Meaning:** A natural or legal person, public authority, agency or any other body (2) / any individual (1) to whom data are disclosed (2) or made available (1) to whom the data may be disclosed (1) Any person entitled to receive communication of such data (1)	**Significant difference.** • Is the recipient the person to whom the data **are** disclosed, or person to whom the data **may be** disclosed / person **entitled** to receive communication of such data? This is quite different. • Different frameworks omit different actors from being a recipient.	

		Other than the data subject, the data controller, the sub-contractor/data processor and persons who for reasons/by virtue of their functions are responsible for processing the data (2) Does not include public authorities which may receive personal data in the framework of a particular enquiry. (1)		
Supervisory authority	9 - All bar UN Guidelines	**Some commonality.** **Term used:** Supervisory authority (4) / privacy enforcement authority (2) / control/supervision authority (1) / national personal data protection authority (1) / authority of protection (1) **Meaning:**	**Some difference.** • The term varies and is not universally used across frameworks. • Only three frameworks specify a 'public' body or authority. • Some frameworks give further detailed requirements in the definition – e.g. that they have	

		Any public body (2) / authority (5) / independent public authority (1) / independent administrative authority (1) responsible for/in charge of enforcing privacy laws (2) / ensuring compliance with/supervising the observance of/ensuring that personal data is processed in compliance/accordance with the principles/provisions.	powers to conduct investigations or pursue enforcement proceedings. Others do not include this in the definition itself. • Only two frameworks specify in the definition that a supervisory authority must be 'independent.' Others do not include this in the definition itself, although eight frameworks elsewhere in the text explicitly require a supervisory authority to be independent, and the other two imply it.	
Sensitive data	7 – all bar OECD; APEC Privacy Framework; UN Guidelines	**Substantial commonality.** **Term used:** Sensitive personal data (1) / sensitive data (3) / special categories of data (2)	**Some difference.** • Data 'revealing' or 'relating to' shows a slight difference in emphasis.	

		/ special categories of personal data (1) **Meaning:** Data that affects the data subject/holder's most intimate sphere or may give rise to discrimination or serious risk (2). Includes data revealing (5) / relating to (3): Racial or ethnic origin (7) Political opinions (7) Trade union affiliation / membership (5) Religious or philosophical beliefs (7) Health (7) Sex life (7)	• Some frameworks describe the term as data that may give rise to discrimination or serious risk, others do not. • Most frameworks specifically include race, political opinions, religious beliefs, health and sexual life. However, criminal proceedings/convictions, genetic/biometric data to identify a person, and social measures are less commonly found.	

		Criminal proceedings and convictions (4) Genetic data or biometric data aimed at identifying a person (2) Social measures (2)		
Profiling	2 – C108+; GDPR	**Some commonality.** **Term used:** Profiling (2) **Meaning:** An automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. (1)	**Some difference.** • Only two frameworks define 'profiling'. • While not inconsistent, the definitions are different in that only one refers to 'particularly in order to take decisions'. • Both agree that profiling includes analysing or predicting, though one is more general, relating this to 'personal preferences, behaviours and	The process of compiling a profile of a person's physical or psychological characteristics.

		Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (1)	attitudes'. The other specifies aspects concerning performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.	
Anonymisation	3 – C108+; Ibero-American Standards; GDPR	**Some commonality (in meaning).** **Term used:** Anonymization (1) / anonymous information (1) **Meaning:** Anonymization: the application of measures of any kind aimed at preventing the identification or re -	**Some difference (in approach).** • Only three frameworks could be said to define 'anonymisation', and some of that is indirect meaning rather than strict definitions. • One framework defines anonymization as a process or application of measures, others as a way of describing the data.	The process of removing names and other identifying features; to make anonymous.

		identification of an individual without disproportionate efforts. Anonymous information: information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. (1) Data is anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, taking into consideration the available technology at the time of the processing and technological developments.	• Apart from the approach however, there are no significant inconsistencies in the general implication of the meanings.	
Pseudonymisation	3 – C108+; Ibero-American	**No commonality (in approach).** **Term used:**	**Some difference (in approach).**	

	Standards; GDPR	Pseudonymisation (1) / pseudonymous data only indirectly defined **Meaning:** Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	• Only one framework actually defines the term; two others do so indirectly. Comparison is therefore difficult.	
Consent	6 – Madrid Resolution; C108+; Ibero-American Standards;	**Substantial commonality.** **Term used:**	**Some difference.** • Some frameworks give further detailed requirements in the	To agree, give permission, accept the actions or opinions of another.

	African Union Convention; GDPR; ECOWAS	Consent **Meaning:** Expression/manifestation of free (5) / freely given (1) / specific (5) / unambiguous (3) / unequivocal (3) / informed (6) / express (2) will (3) / indication of the data subject's wishes (1) By a statement or clear affirmative action (2) Through which the data subject accepts (4)/authorizes (1)/signifies agreement to (1) the processing.	definition / wider description of the concept, e.g. the Madrid Resolution includes a requirement for consent to be withdrawable at any time, Convention 108+ clarifies that consent can be given in written, electronic or oral form.	
Personal data breach	4 – OECD; C108+; Ibero-American Standards; GDPR	**Substantial commonality** **Term used:**	**Some difference.**	

		Personal data breach / data breach / security breach **Meaning:** A breach / violation of the security / safety of personal data, leading to / understood as accidental (3) / unlawful (1) damage (1), loss (4), modification/alteration (4), destruction (4), unauthorised disclosure of, or access to, (4) personal data.	• Only four frameworks define the term, and two of those do so indirectly.	
Transborder flows of personal data	3 – OECD; C108; C108+	**Some commonality.** **Term used:** Transborder flows of personal data (2) / transborder data transfer (1)	**Some difference (in approach).** • Only three frameworks define the term. • Two describe the term as personal data being moved / transferred across borders,	

		Meaning: Movements of personal data across borders (2) by whatever medium (1) / occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation (1)	although one of these clarifies by whatever medium, whereas one describes the term as personal data being disclosed/made available to a recipient subject to another jurisdiction.	
Accountability	6 – Madrid Resolution; OECD; APEC Privacy Framework; C108+; Ibero-American Standards; GDPR	**Some commonality.** **Term used:** Accountability (5) **Meaning:** Implementing measures / mechanisms to comply with (5) being able to demonstrate compliance with (3) the principles/obligations.	**Some difference.** • No formal definitions, all frameworks that describe the term do so informally. • Some frameworks specify who controllers should be accountable to – to supervisory authorities (3) and data subjects (2). Others do not. • Some frameworks give examples of how accountability	The fact or condition of being accountable; responsibility; being able to give a satisfactory reason for actions.

			can be ensured / demonstrated, such as the use of privacy management programmes. Others do not.	
Transparency	7 – all bar C108; African Union Convention; UN Guidelines	**Some commonality.** **Term used:** Transparency (4) / openness (2) / notice (1) **Meaning:** Informing / providing information / openness about the processing of personal data.	**Some difference.** • 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. • Some frameworks provide much more detailed requirements as to what constitutes transparency, setting out specific items of information that should be provided.	Openness.

Data protection/privacy by design and default	5 – Madrid Resolution; OECD; C108+; Ibero-American Standards; GDPR	**Some commonality (of meaning).** **Term used:** Privacy by design (1) / privacy due to design and privacy by default (1) / data protection by design and by default (1) **Meaning:** Technologies, processes and practices are built into system architectures, rather than added on later as an afterthought / processing is designed in such a manner as to prevent or minimise the risk of interference with […] rights and fundamental freedoms / the application of preventive measures that allow the effective application of principles, rights and obligations / at the time of determining the means for processing and at the time of the processing itself, the implementation of appropriate technical and	**Some difference (in wording – although general meaning is consistent).**	

		organisational measures […] designed to implement the data protection principles.		
Data protection / privacy impact assessment	4 – OECD; C108+; Ibero-American Standards; GDPR	**Some commonality (of meaning).** **Term used:** Privacy impact assessment / impact assessment on the protection of personal data / data protection impact assessment **Meaning:** A process of analysing and evaluating the risks to individuals' privacy. Should be carried out before a new programme or service is introduced, or where the context of data use has changed significantly.	**Some difference (in wording – although general meaning is consistent).**	

		An examination of the likely impact of intended data processing on the rights and fundamental freedoms of data subjects. An assessment of the impact of the envisaged processing operations on the protection of personal data . The assessment should contain a description of the envisaged processing operations and the purpose for the processing, an assessment of the necessity and proportionality of the processing in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, and the measures to address the risks.		

Privacy management programme	2 - OECD; APEC Privacy Framework	**Substantial commonality.** **Term used:** Privacy management programme **Meaning:** An operational mechanism through which organisations implement privacy protection and demonstrate compliance.	**Some difference.** • Only two frameworks describe the term, both indirectly without a formal definition.	
Binding corporate rules	2 – Madrid Resolution; GDPR	**Substantial commonality.** **Term used:** Binding corporate rules / internal privacy rules	**Some difference.** • Only two frameworks describe the term, both indirectly. • GDPR describes the term in more detail – for example	

		Meaning: Legally binding/mandatory internal rules that apply to, and are enforced within, corporations or multinational groups, to enable cross-border transfers of personal data.	that the rules should confer enforceable rights on data subjects.	

Appendix 3: Privacy and data protection terms, and their meanings

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
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.**