Policy Strategy Working Group 1: Global frameworks and standards

Report – adopted October 2020

Chair authority: UK ICO

Table of Contents Page

Executive Summary

The adoption of the Resolution on the Conference's strategic direction, including the new Policy Strategy, in Tirana in 2019 was a pivotal moment, setting out a new level of ambition in transforming the GPA into a year-round assembly for regulatory cooperation, adding value to global debates around privacy and data protection.

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

PSWG1's work in 2019-20 has therefore focused on delivering the Policy Strategy action to complete an analysis of current global frameworks for privacy and data protection, including key principles, data subject rights, cross-border transfers, and demonstrable accountability standards.

Ten global frameworks from across all GPA regions were analysed:

- 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
- ECOWAS Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

The criteria used to analyse the frameworks were selected in order to fulfil the requirements of the mandated action – to include "key principles, data subject rights, cross-border transfers and demonstrable accountability standards." It is the first time all these frameworks have been assessed together by the GPA.

While the nature and scope of the frameworks differed to varying degrees, headline results showed that there were very strong commonalities between the frameworks, particularly around a significant number of core principles and data subject rights, and other requirements such as the role of independent supervisory authorities. These are set out on page 8 of this report. PSWG1 believes that highlighting the strong degree of commonality and convergence between the frameworks, and setting out the common fundamental principles and core elements in a referential document, will assist GPA members by providing an evidence base which emphasises the importance of the common elements found. The referential document can be found in Annex 2.

The referential document would not only suggest a commitment to shared values between the frameworks and the GPA members who work within them, but could also provide a point of

reference for GPA members in their conversations with those they regulate, their governments and wider global stakeholders.

PSWG1 will then consider in 2020-21 how to create a narrative or policy statements based on this analysis work, including what the long term value of this output can be to the GPA, both to its own work and to its interaction with external developments and institutions. This will also allow more time to hear member feedback on that aspect of the forward looking plan and what the level of ambition for the GPA should be, building from the platform of evidence now collated. It will also enable PSWG1 to consider further analysis of the key features of independent privacy and data protection authorities, drawing from the GPA census (which has been delayed due to COVID-19).

In one part of the analysis in particular, findings relating to cross-border transfers indicated that while there are broadly similar general principles around the need to protect personal data across-borders, there are a variety of different mechanisms in use. These mechanisms themselves require further analysis in order to reach any substantive conclusions. PSWG1 has therefore recommended carrying out further analysis work on cross-border transfers in 2020-21.

Other work planned for 2020-21 includes delivery of Policy Strategy Pillar 1, action 2, to consider developing common definitions of key data protection terms.

Introduction

The adoption of the Resolution on the Conference's strategic direction[1] at the 41st ICDPPC (now GPA) conference in Tirana in 2019 created the GPA strategic plan for 2019-21 and included the first GPA Policy Strategy. The Policy Strategy highlighted a new level of ambition for the GPA as it aimed to transform into a year-round assembly that added real value to privacy and data protection debates, with a clear focus on regulatory cooperation.

Policy Strategy Working Group 1 (PSWG1) was established subsequent to the adoption of the resolution and derives its mandate from it. PSWG 1 is responsible for delivering an element of the Policy Strategy relating to the GPA's first Strategic Priority for 2019-21 – 'Work towards a global regulatory environment with clear and consistently high standards of data protection'; more specifically Pillar 1 of the Policy Strategy, namely 'Global frameworks and standards' and the 'evolution towards global policy, standards and models for data protection and privacy'.

There are two Pillar 1 Policy Strategy actions, forming the first steps towards that evolution, as follows:

- Pillar 1, action 1 – Complete an analysis of current global frameworks for privacy and data protection, including key principles, data subject rights, cross-border transfers and demonstrable accountability standards.
- Pillar 1, action 2 – Consider developing common definitions of key data protection terms.

PSWG1's work plan set out that the group would address action 1 in 2020, and action 2 in 2021. All work done in 2020 has therefore been focused on delivering action 1. PSWG1 has met four times, engaging in addition when required via email. This has enabled the group to fulfil its mandate for 2020 with the analysis of global frameworks completed.

2019-20 also saw the creation of the ExCo Strategic Direction Sub-Committee (SDSC) to coordinate and review the Policy Strategy actions. The PSWG1 Chair attended a meeting of the SDSC on 18 June 2020, to set out the 2020 work plan and describe activities carried out and progress made against the Policy Strategy actions so far. SDSC members were satisfied that appropriate progress was being made, and suggested that the output should be socialised and evaluated to assess how widely it is used. PSWG1 agreed to ensure this featured in the future work plan as outputs are delivered.

Working Group members

UK ICO (Chair)	Council of Europe	EDPS	CNIL France	Gabon
Germany BfDI	Israel	Korea PIPC	INAI Mexico	NPC Philippines
San Marino	Switzerland FDPIC	Turkey	US FTC	Uruguay
Dubai International Financial Centre Authority (observer)		European Commission (observer)		EDPB (observer)

[1] Resolution on the Conference's strategic direction 2019-21

Working Group Activities

Analysis of current privacy and data protection frameworks

In 2020, PSWG1 focused on delivering the analysis in Pillar 1, action 1 of the Policy Strategy, to "Complete an analysis of current global frameworks for privacy and data protection, including key principles, data subject rights, cross-border transfers and demonstrable accountability standards."[2]

Methodology

At its first meeting in January 2020, the group agreed its terms of reference and the methodology to be followed in carrying out the analysis. It was agreed that ten frameworks would be analysed, covering all the regions of the GPA. The ten frameworks compared were:

- 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
- ECOWAS Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

The ten frameworks were analysed according to a long list of criteria. The criteria used to analyse the frameworks were selected in order to fulfil the requirements of the mandated action – to include "key principles, data subject rights, cross-border transfers and demonstrable accountability standards."

The analysis was desk-based and involved researching the framework texts themselves, as well as a number of academic and legal publications. Searches were carried out for previous exercises and articles in a substantively similar vein. None appeared to undertake as broad a comparison of frameworks but a number of previous and current exercises were noted:

- Greenleaf, Graham (2011), Global data privacy in a networked world.
- United Nations Conference on Trade and Development (UNCTAD) (2016), Data protection regulations and international data flows: Implications for trade and development.
- Consumers International (2018), The state of data protection rules around the world: A briefing for consumer organisations.
- A number of law firms have carried out, and carry out on an ongoing basis, comparisons of data protection laws in countries across the world, the most extensive of which is DLA Piper (2020) Data Protection Laws of the World Handbook.

[2] Resolution on the Conference's strategic direction 2019-21, page 7

The full, completed data table comparing all ten frameworks in relation to the criteria can be found in Annex 1.

Headline similarities and differences identified

1. **Nature and scope of the frameworks**

It was noted that the nature of the frameworks themselves was varied. Some are binding, such as the EU General Data Protection Regulation (GDPR), the ECOWAS Supplementary Act and Convention 108. Others will enter into force and become binding when the minimum number of signatories/member states ratify the instrument, such as Convention 108+ and the African Union Convention. Others are sets of principles and guidelines, such as the APEC Privacy Framework, the Ibero-American Standards and the OECD Guidelines. Variations in nature and scope mean that although frameworks may include particular principles, rights and other elements, the level of protection provided by each framework will not always be equivalent.

There are some consistent similarities in scope across many of the frameworks, for example:

- Application across both **public and private sectors** to at least some degree.
- Application to fairly consistent definitions (where definitions exist) of the **processing of personal data.**
- Non-application to personal data processed by individuals for **domestic or household purposes.**

2. **Key principles to be applied to the processing of personal data**

There is, in the main, broad agreement on key principles across the frameworks. The following principles are all notable for their consistent appearance in all, or a significant majority of, frameworks:

- **Fairness** – all frameworks set out that personal data should be processed fairly, although few definitions as to what is meant by 'fairness' are offered. Links are made with non-discrimination, transparency, as well as the avoidance of deceit or fraud.
- **Lawfulness** – nearly all frameworks set out that personal data should be processed lawfully. Only some, however, go on to specify legitimate bases or conditions for processing to be considered lawful or legitimate.
- **Purpose specification** – all frameworks include some variation of the requirement that personal data should be processed only for specified, defined, explicit and legitimate purposes.
- **Proportionality** – this principle is included in all frameworks, although to varying degrees, from specific data minimisation requirements, some general requirements of proportionality, specific requirements of non-excessive processing of personal data through to broader requirements of relevance to purpose.
- **Data quality** – requirements to keep personal data accurate, complete and up to date appear consistent across frameworks.

- **Openness/transparency** – the inclusion of some degree of openness or transparency can be found in all frameworks. Degrees range from general requirements to have transparent policies, and to ensure information about personal data processing is made available, to specific lists of information that must be provided directly to data subjects.
- **Security** – this is another consistently used principle, with all frameworks setting out requirements for appropriate (or sufficient) measures to be in place.
- **Data retention** – almost all frameworks require data to be retained only for as long as is necessary for the purposes of processing. Some frameworks make special provision for data processed for archiving or research purposes to be retained for longer periods.
- **Accountability** – the inclusion of accountability as a general principle is slightly less generally seen, with six out of the ten frameworks requiring that data controllers (and where applicable, processors) are accountable for the personal data they process and, crucially, in most of them, that they are able to demonstrate or prove compliance.

The comparison indicated that there is a high degree of commonality across the frameworks where the general principles above are concerned, perhaps reflecting an almost universal acceptance of their importance in protecting personal data.

There appears to be slightly less agreement where **accountability** as a principle is concerned, particularly in the older instruments and in the two African frameworks analysed. It would be useful to understand any reasons for the latter.

3. Data subject rights

Again, for some data subject rights there appears to be a high degree of commonality across all, or nearly all, frameworks.

- **Access** – the right of access is universally acknowledged across all frameworks, linked in some cases to allowing the data subject to evaluate and contest the processing if necessary.
- **Objection/opposition** appears in six out of the ten frameworks.
- **Rectification** is a point of similarity across all frameworks, often linked to, and following on from, the right of access, when data is found to be inaccurate.
- **Deletion/erasure** is another universally accepted right, albeit with differences in scope.. Some frameworks link this right to inaccurate or out of date data; however others allow the data subject to request deletion for a broader set of reasons.

Rights of **restriction** and **data portability** are much less generally seen. Only the Ibero-American Standards and GDPR appear to explicitly include these rights.

There is a fairly even split where rights around **automated decisions** are concerned, with four frameworks including such rights (Convention 108+, Ibero-American Standards, GDPR and ECOWAS Supplementary Act) and the remaining six frameworks not doing so. As the potential for increased numbers of automated decisions, for a broader range of purposes, grows, along with wider deployment of newer technologies such as AI, this might be a gap to consider further.

4. Accountability standards

While six out of ten frameworks include a general accountability principle, the number of frameworks specifying particular standards for controllers to demonstrate accountability tend to be fewer. Only the Madrid Resolution, the Ibero-American Standards, Convention 108+ and GDPR specify **data protection officers**, **training** and **audits** as accountability measures. **Breach prevention, response plans and reporting** are only specified to varying extents by these same four frameworks, plus the APEC Privacy Framework and OECD Guidelines.

Again, some common ground is to be found in relation to **privacy by design** and, in particular, **privacy/data protection impact assessments** – with a fairly even split between those frameworks that include the measures and those that do not.

Codes of conduct/practice and **records of processing activities** are less well supported, as only three frameworks explicitly include the former and only one the latter.

There may be some scope for further thought around any risks posed by these gaps – in particular in relation to **breach response plans and reporting**, as well as **impact assessments**, as these seem more widely accepted for inclusion in the frameworks.

5. **Specific themes and requirements**

Almost all frameworks set out specific requirements for **sensitive personal data**, bearing in mind the increased risks posed by its processing. Other specific themes that appear in far fewer frameworks include **processors**, **joint controllers**, **professional secrecy** and **access to data by public authorities**.

Only three frameworks include specific requirements for the processing of personal data of **vulnerable groups and/or children**. This seems surprising given the increased interest in safeguards around the processing of children's data in recent years, and could be an omission worth considering further.

6. **Compliance and monitoring**

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. Bearing in mind the GPA requirement for an independent supervisory authority in new GPA member applications, this could be a gap to consider further.

Most frameworks make some reference to **cooperation with other authorities** within their framework membership, but only four frameworks make any mention of cooperation with other authorities outside or between frameworks, the latter often in relation to encouraging the development of mechanisms for cooperation more widely. Bearing in mind increasingly global levels of processing, this might be a gap to consider further.

Redress, **fines** and **penalties** all see fairly even splits between those frameworks that include provisions and those that do not, although slightly more frameworks do include such provisions.

7. **Cross-border transfers**

All frameworks except the African Union Convention include **general principles on cross-border transfers**. The general approach in these principles is that transfers can take place if appropriate levels of protection are in place.

Some frameworks specify different approaches for transfers between members, and between members and non-members. An example of this is GDPR, which assumes that transfers between member states need no further consideration, but which specifies a number of mechanisms available to use for transfers to 'third countries' outside the EU.

Further, some frameworks set out clear mechanisms for transfers, whilst others do not.

Whilst seven out of the ten frameworks could be said to imply a notion of **adequacy** where they suggest that appropriate levels of protection for transfers can be based on state laws, only GDPR specifies a mechanism for assessing the adequacy of regimes outside the EU.

Adequacy is the only mechanism specified in the ten frameworks that can be applied to whole states. Other mechanisms tend to focus on narrower arrangements. **Approved self-assessment schemes for organisations** include, for example, the APEC Cross-Border Privacy Rules System. Whilst the Ibero-American Standards also refers to the possibility of assessing particular sectors, activities, international organisations or recipients to enable transfers to take place, no mechanism is specified.

Two frameworks (the Madrid Resolution and GDPR) specifically refer to **internal privacy rules/binding corporate rules** as a mechanism for obtaining guarantees/safeguards for transfers within multinational corporations.

Whilst GDPR again refers to specific **contractual clauses** that can be used as a mechanism between different organisations to transfer personal data across-borders, three other frameworks make a general reference to them.

Codes of conduct, **certification** and **administrative arrangements** all receive little attention from frameworks other than GDPR in terms of cross-border transfers (although the Ibero-American Standards do refer to certification).

Conclusions and next steps

It was clear from the analysis that there is broad agreement across the frameworks in terms of key principles, a number of core rights and other requirements, and in particular around the role of supervisory authorities. The similarities identified could, as a starting point, assist GPA members by providing an evidence base which emphasises the importance of the common elements found.

In considering what next steps could add most value to the work, a number of options were considered but the group concluded that as the mandate for 2020, i.e. the completion of the analysis, had been fulfilled it would be appropriate to deliver an output for 2020 which highlighted the strong degree of commonality and convergence found between the frameworks. This output would not only suggest a commitment to shared values between the frameworks and the GPA members who work within them, but could also provide a point of reference for GPA members in their conversations with those they regulate, their governments and wider global stakeholders. This referential document can be found in Annex 2.

Findings relating to cross-border transfers indicated that while there are broadly similar general principles around the need to protect personal data across-borders, there are a variety of different mechanisms in use. These mechanisms themselves require further analysis in order to reach any substantive conclusions. PSWG1 has therefore recommended carrying out further analysis work on cross-border transfers in 2020-21.

Forward looking plan 2020-2021

The following actions have been identified for PSWG1 to deliver in 2020-21:

- Next steps in the form of further output from the global frameworks analysis: PSWG1 will explore whether a resolution or other policy outputs aimed at external stakeholders highlighting the value of the convergence identified, and the core common elements of data protection and privacy frameworks, will enhance the delivery of the policy strategy. It will also enable PSWG1 to consider further analysis of the key features of independent privacy and data protection authorities, drawing from the GPA census (which has been delayed due to COVID-19). Further analysis of government and public authority access to personal data could also be considered. The completed analysis did not highlight any particular issues around this topic but it complements the other actions and is of current interest to a number of GPA members.
- An analysis of cross-border transfer mechanisms, how they enable transfers while protecting personal data across-borders, how they are used in practice, and areas of commonality/difference. This could include surveys and interviews with those who use them as well as desk-based research. This could in turn involve engaging outside the GPA, for example with the new GPA Reference Panel representatives. A report on cross-border transfers could then be prepared, addressing what value the GPA could add in addressing the findings.
- Pillar 1, action 2: Reflecting the need for a common global language for data protection and privacy, both within the GPA as a reference point and to enhance capacity building, and externally to influence global debates, commence a rolling programme to develop common definitions of what is meant by key data protection terms, such as accountability. This will involve an analysis of key data protection terms currently defined across different frameworks and in particular any differences and any reasons why these differences might exist. It will also involve identifying those key data protection concepts for which agreed definitions do not currently exist, and considering the value and practicality of developing common definitions for particular terms. The aim would be to start with a core set of terms that could be readily agreed and built on over time, recognising the importance of consensus.

PSWG1 notes the need to be aware of developments in the OECD's review of its Privacy Guidelines, and will engage with OECD in relation to the above actions in order to avoid duplication, and to influence where appropriate.

Conclusion

In the first year of its existence, PSWG1 has delivered its planned actions for 2019-20 by completing the global frameworks analysis. In delivering the referential document, PSWG1 has highlighted its findings in a way that adds value by providing a good evidence base for GPA member authorities to use in their conversations with those they regulate.

The Strategic Plan and Policy Strategy continue into 2020-21, and in the second year PSWG1 aims to complete the rest of its allocated actions, by further analysing cross-border transfer mechanisms, and considering developing common definitions of data protection terms.

Annex 1: Analysis of current privacy and data protection frameworks: data table

Policy Strategy Working Group 1: Global frameworks and standards

Analysis of current privacy and data protection frameworks: data table

This table sets out the data collected in PSWG1's analysis of current frameworks for privacy and data protection, including key principles, data subject rights, cross-border transfers and demonstrable accountability standards. Data has been collected in relation to the following ten frameworks:

- 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
- ECOWAS Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

The criteria used to analyse the frameworks are those in the left-hand columns of the table. These criteria are intended to fulfil the requirements of the action we have been tasked with – to include "key principles, data subject rights, cross-border transfers and demonstrable accountability standards."

Comparison table – global frameworks and standards: principles, rights and accountability standards

	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
Number of parties	Members of the 31st ICDPPC, Madrid Spain 2009.	34 members	21 APEC member economies	55 (47 CoE member states ratified, 8 non-CoE members acceded)	5 member states ratified and 36 signed to date	23 member states (Ibero-American Network on Data Protection)	14 countries signed, 5 ratified	27 members	193 current member states	15 current member states
Stated aims/ objectives, if any	To define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data:		- Promoting e-commerce throughout the Asia-Pacific region. -Encourage the developme-nt of appropriat e privacy protections and	To secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and	To protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal	- To establish a set of data protection principles and rights, for States to adopt and develop in their legislation. - To raise protection of individuals, and	To address the need for harmonized legislation in the area of cyber security in Member States and to establish in each state party a mechanism to combat	**Recital 2** – to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic		**Article 2: Aims** Each Member State shall establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of

	and the facilitation of the international flows of personal data needed in a globalised world.		ensuring the free flow of information in the Asia Pacific region.	fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to his "data protection".	data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.	guarantee the effective exercise of data protection rights of any person in the Ibero-American States, by establishing common rules. - Facilitate the flow of personal data between Ibero-American States and beyond their borders. - To drive the development of mechanisms for international cooperation.	privacy violations. To guarantee that processing shall respect basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses. To take on board internation-ally recognised best practices. State parties shall commit to establishing a legal	and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.		personal data without prejudice to the general interest of the State.

							framework aimed at strengthening fundamental rights and public freedoms.			
Scope / application										
Binding law or guidelines / principles?	A joint proposal for a draft of international standards.	Guidelines – should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual	A set of principles and guidelines – to be implemented as each member economy determines. The framework states there should be flexibility in implementing the principles,	International convention – binding when ratified.	International convention – binding when ratified. Provisional application is possible upon declaration (as declared by Bulgaria,	A set of guidelines / standards that States can adopt in development of new and existing legislation. Flexible enough to be adopted without contravening member state laws.	Convention – adopted by the Assembly of the African Union. Will not enter into force until 15 member states have ratified the Convention (to date only 5 states have ratified).	A European Union Regulation, applicable across all member states.	Guidelines – a UN resolution adopted revised guidelines in December 1990. UN General Assembly request for governments to take the guidelines into account in their law	Supplementary Act to the ECOWAS Treaty – binding on Member States.

		liberties, which may impact transborder flows of personal data.	in view of different social, cultural, economic and legal backgrounds of member economies.		Lithuania and Norway[3]). Partial entry into force possible from 2023 with 38 ratifications (full entry into force when all Parties to Convention 108 will have ratified).				and regulations.	
Material scope	Any processing of personal data, wholly or partly by automatic means, or otherwise in a structured manner and	Guidelines apply to personal data, whether in the public or private sectors, which,	Applies to the collection, holding, processing, use, transfer or disclosure of personal information about	Applies to the automated processing of personal data in both public and private sectors. Parties can	Applies to the processing of personal data in both public and private sectors,	Applies to the treatment of personal data of individuals contained in physical, fully or partially or both, automated	Applies to any collection, processing, transmission, storage or use of personal data by a natural person, the	**Article 2** The Regulation applies to the processing of personal data, either wholly or partly by	**Field of application** Principles should be applicable to all public and private computerized files as well as, by means	**Article 3: Scope** Collection, processing, transmission, storage, and use of personal data by any individual, by

[3] See : https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/declarations?p_auth=h61bPRI5

	carried out in both the public and private sectors, subject to each Party's jurisdiction.	because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties. In federal countries the observance of these Guidelines may be affected by the division of	natural living persons. Limited application to publicly available information.	declare the Convention does not apply (exclusion) or it does apply (extension) to certain categories of files.	subject to each Party's jurisdiction. It does not apply to data processing carried out by an individual in the course of purely personal or household activities.	media, regardless of the form or modality of their creation, type of media, processing, storage and organization.	State, local communities, and public or private corporate bodies. Any automated or non-automated processing of data contained in or meant to be part of a file.	automated means, and to non-automated processing of personal data which form part of or are intended to be part of a filing system. Does not apply to the processing of personal data for activities falling outside the scope of EU law such as: (a) in the course of an activity which falls outside the scope of Union law;	of optional extension and subject to appropriate adjustments, to manual files. States can opt to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.	government, local authorities, and public or private legal entities shall be subject to this Supplementary Act.

		powers in the federation.						(b) for purely personal and household activities; (c) by competent authorities for criminal investigation, detection, prosecution.		
Scope includes private sector and public authorities, including government? **National security?**	Both private and public sectors. Restrictions in the interests of national security, public safety, protection of public health or rights and freedoms of other should be expressly	Both private and public sectors. Exceptions to the Guidelines should be as few as possible but may relate to national sovereign-	Framework – both private and public sectors, however it should be noted that: - it is not intended to impede government activities authorized by law when taken to protect	Both private and public sectors. Derogation from certain articles allowed when provided for by the law of the Party and	Both private and public sectors. Exceptions allowed to certain Articles when such an exception is provided for by law,	Both public and private sectors. Standards apply to individuals, private legal entities, authorities and public bodies. National legislation may limit the	Both public and private sectors. Applies to any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities,	Both private and public sectors. Does not apply to issues which fall outside the scope of EU law, e.g. national security.	Both private and public sectors. Principle 6: Power to make exceptions. Departures from principles 1 to 4 may be authorized only if they are necessary	Both private and public sectors. Processing […] by any individual, by government, local authorities, and public or private legal entities shall be subject to this

	provided by national legislation.	-ty, national security and public policy ("ordre public").	national security. - the **Cross-Border Privacy Rules System** applies only to the personal data processing of business organizations, not governments or individuals.	constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, protecting the data subject or the rights and freedoms of others.	respects the essence of the fundamental rights and freedoms and constit-utes a necessary and proport-ionate measure in a demo-cratic society for: a. the protection of national security, defence, public safety, important economic and financial	right to the protection of data in order to safeguard national security, public security, public health protection, the protection of rights and freedoms of third parties, as well as due public interest matters. Limitations and restrictions shall be expressly acknowledged in the law.	and public or private corporate bodies. Any processing of data relating to public security, defence, research, criminal prosecution or State security may be subject to exceptions defined by specific provisions of other extant laws.		to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others […]provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.	Supplementary Act. Applies to any processing of data related to public security, defence, investigation and prosecution of criminal offences or State security, subject to such exemptions as are defined by specific provisions stipulated in other legal texts in force.

					interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; b. the protection of the data					

					subject or the rights and fundamental freedoms of others, notably freedom of expression.					
Territorial scope		Member countries are recommended to implement the guidelines, non-Members are invited to adhere to them.	APEC member economies.	**Article 24: Territorial clause** – Any State may at the time of signature / ratification or any later date specify the territory / territories to which the Convention shall apply.	**Article 28: Territorial clause** – Any State, the European Union or other international organisation may, at the time of signature / ratification or any later date	**5. Field of Territorial Application** Standards apply to personal data treated by a person responsible or in charge - established in the territory of the Ibero-American States.	**Article 9: Scope of application of the Convention** – Any processing of data undertaken in the territory of a State Party.	**Article 3** Applies to the activities of a controller or a processor established in the Union, regardless of whether the processing takes place in the		**Article 3: Scope** – any processing carried out in an UEMOA or ECOWAS Member State.

				(Such declaration may also be withdrawn)	specify the territory / territories to which this Convention shall apply. (Such declaration may also be withdrawn).	- not established but where treatment relates to goods and services aimed at residents of the Ibero-American States. - by a person responsible or in charge, not established in the territory but to whom the national legislation of such States applies. - by a person responsible or in charge, not established in the territory but		Union or not. Also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: - the offering of goods or services to such data subjects in the Union.		

						uses means located in such territory, unless only for transit.		- the monitoring of their behaviour as far as their behaviour takes place within the Union. Also applies to processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public internation al law.		

Definitions										
Personal data	'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.	'Personal data' – any information relating to an identified or identifiable individual.	'Personal data' – any information regarding an individual identified or identifiable.	'Personal data' – any information relating to an identified or identifiable natural person.	**Article 4** '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 .
Processing	'Processing' – any operation or set of operations, automated or not, which is performed on personal data, such as collection, storage, use, disclosure or deletion.			'Automatic processing' – includes the following operations if carried out in whole or in part by automated means: storage of data,	'Data processing' – any operation or set of operations performed on personal data, such as the collection, storage, preservati	'Treatment' – any operation or set of operations performed through physical or automated procedures on personal data (includes collection,	'Processing of personal data' – any operation or set of operations which is performed upon personal data, whether or not by automatic	**Article 4** 'Processing' – any operation or set of operations which is performed on personal data or on sets of personal data, whether or		'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

				carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or disseminati on.	on, alteration, retrieval, disclosure, making available, erasure, or destructio n of, or the carrying out of logical and/or arithmetic al operations on such data.	access, registration, organisation, structuring, adaptation, indexation, modification, extraction, consultation, storage, preservation, development , transfer, disseminatio n, possession, exploitation, and, in general any use or disposal).	means, such as the collection, recording, organization, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, disseminatio n or otherwise making available, alignment or combination and locking, encryption, erasure or destruction.	not by automated means, such as collection, recording, organisatio n, structuring, storage, adaptation or alteration, retrieval, consultatio n, use, disclosure by transmissio n, disseminati on or otherwise making available, alignment or combinatio n, restriction,		obtaining, using, recording, organisation, preservation, adaptation, alteration, retrieval, 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.

								erasure or destruction.		
Profiling					**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**[4]:			**Article 4** 'Profiling' - 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 performanc		

[4] https://rm.coe.int/16807096c3

					d. “Profile” refers to a set of data characterising a category of individuals that is intended to be applied to an individual. e. “Profiling” means an automatic data processing technique that consists of applying a “profile” to an individual, particularly in order to take decisions			e at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.		

					concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. (NB not legally binding).					
Pseudonymisation					Not strictly defined, but **Article 18** of the **Explanatory Report** refers to 'pseudonymous' data.	Not strictly defined, but **Article 2.1.a** defines anonymization broadly, as 'the application of measures of any kind aimed at preventing the identification or re-		**Article 4** 'Pseudonymisation' – the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject		

						identification of an individual without disproportionate efforts.'		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.		
Controller	'Responsible person' – means any natural	'Data controller' – a party who,	'Personal information controller' – person or	'Controller of the file' – the natural or legal	'Controller' – the natural or legal	'Person responsible' – individual or legal	'Data controller' – any natural or legal	**Article 4** 'Controller' – the natural or		'Data controller' means any public or

	person or organization, public or private, which alone or jointly with others, decides on the processing.	according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.	organisation who controls, or instructs another, to collect, hold, use, process, transfer or disclose personal information.	person, public authority, agency or any other body who is competent according to the national law to decide 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.	person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing.	private entity, public authority, services or body that, alone or together with others, determines the purposes, means, scope and other matters related to the treatment of personal data.	person, public or private, any other organization or association which alone or jointly with others, decides to collect and process personal data and determines the purposes.	legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.		private individual or legal entity, body or association who, alone or jointly with others, decides to collect and process personal data and determines the purposes for which such data are processed.
Processor	'Processing service provider' – means any				'Processor' – a natural or legal	'Person in charge' – a service provider	'Sub-contractor' – any natural or legal	**Article 4** 'Processor' – a natural or legal		'Data processor' – any public or private

	natural person or organisation, other than the responsible person that carries out processing of personal data on behalf of such responsible person.				person, public authority, service, agency or any other body which processes personal data on behalf of the controller.	(individual, legal entity or public authority) that treats personal data on behalf of the person responsible.	person, public or private, any other organization or association that processes personal data on behalf of the data controller.	person, public authority, agency or other body which processes personal data on behalf of the controller.		individual or legal entity, body or association who processes personal data on behalf of the data controller.
Third Party							‘Third party’ – a natural or legal person, public authority, agency or body, other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller	**Article 4** ‘Third party’ – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct		‘Third party’ – any public or private individual or legal entity, body or association other than the data subject, the data controller, the data processor and any other persons placed under the direct authority of

							or the processor are authorized to process the data.	authority of the controller or processor, are authorised to process personal data.		the data controller or the data processor, who is authorised to process data.
Recipient					'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,	**Article 4** '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		'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.	which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law.		
Consent	Personal data may only be processed after obtaining the free, unambiguous and informed consent of the data subject. The responsible person shall provide simple, fast and efficient procedures				**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 of the data subject or	'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 concern him.	'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 representative accepts that his/her personal data be subjected	**Article 4** '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		'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 processed either

	that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor gain for the responsible person.				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 must represent the free expression of an intentional choice, given		to manual or electronic processing.	affirmative action, signifies agreement to the processing of personal data relating to him or her.		manually or electronically.

					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						Defined in **Article 22.1** as 'a violation to the safety		**Article 4** 'Personal data breach' – a		

						of personal data.. ..understood as any damage, loss, alteration, destruction, access and, in general, any illegal or non-authorized use of personal data, even if it occurs accidentally.'		breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.		
Supervisory Authority		'Privacy enforcement authority' – any public body, as determined by each Member country, that is	'Privacy Enforcement Authority' – any public body responsible for enforcing privacy laws and that has powers to investigate	**Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing**	**Article 15** Each Party shall provide for one or more authorities to be responsible for ensuring complianc	Not fully defined but clearly referred to in **Article 42** : 'Nature of Control and Supervision Authorities'		**Article 4** 'Supervisory authority' – an independent public authority which is established by a Member State		'Authority of Protection' – the data protection authority shall be an independent administrative authority responsible for ensuring that personal

		responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings.	and enforce.	**of Personal Data regarding supervisory authorities and transborder data flows:** **Article 1** Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention	e with the provisions of this Convention.			pursuant to Article 51.		data is processed in compliance with the provisions of this Supplementary Act.

				and in this Protocol.						
Key principles										
Principles: **Fairness**	**Principle of lawfulness and fairness** – Personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedoms of individuals as set out in the Resolution and in conformity with the purposes and principles of the Universal Declaration of Human Rights	7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of	**Collection limitation principle** – Information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.	**Article 5: Quality of data** – Personal data shall be obtained and processed fairly and lawfully.	**Article 5: Legitimacy of data processing and quality of data** – Data processing shall (…) reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the	**15. Loyalty principle** – The person responsible shall treat personal data - protecting the holders' best interest. - refraining from treating the data through deceiving or fraudulent means. Treatment that results in unfair or arbitrary discrimination against	**Article 13, Principle 2: Principle of lawfulness and fairness of personal data processing** – The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently.	**Article 5(1)(a): Lawfulness, fairness and transparency principle –** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.	**Principle of lawfulness and fairness** – information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.	**Article 24: Principle of legality and fairness** – The collection, recording, processing, storage, and transmission of personal data must be carried out in a legal, fair and non-fraudulent manner.

	and the International Covenant on Civil and Political Rights. Processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.	the data subject.			rights and freedoms at stake. Personal data undergoing processing shall be processed fairly and in a transparent manner.	holders shall be considered unfair.				
Principles: **Lawfulness (including legal/lawful bases for processing)**	**Principle of lawfulness and fairness** – Personal data must be fairly processed, respecting the applicable national legislation as well as the rights and freedoms as set out in the	7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair	**Collection limitation principle** – information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the	**Article 5: Quality of data** – Personal data shall be obtained and processed fairly and lawfully.	**Article 5: Legitimacy of data processing and quality of data** – Personal data undergoing processing shall be	**11. Legitimation principle** – Person responsible can only treat personal data if: - holder consents - necessary for	**Article 13, Principle 1: Principle of consent and legitimacy of personal data processing** – Processing will be deemed legitimate where the data subject	**Article 5(1)(a): Lawfulness, fairness and transparency principle –** Personal data shall be processed lawfully, fairly and in a	**Principle of lawfulness and fairness** – information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends	**Article 23: Principle of consent and legitimacy** – processing is legitimate where the data subject has given consent. Consent requirement can be waived

	Resolution in conformity with the purposes and principles of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights Processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair. Processing of personal data is necessary for the maintenance	means and, where appropriate, with the knowledge or consent of the data subject.	individual concerned.		processed lawfully. **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 of the data subject or of some other legitimate basis laid down by law.	compliance with court order, resolution, competent public authority mandate - necessary for exercise of public authority powers - necessary for defence of holder's rights before a public authority - necessary for agreement/ pre-agreement - necessary for compliance with a legal obligation	has given his/her consent, or where the processing is necessary for: - controller's compliance with a legal obligation - performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or a third party - performance of a contract to which the data subject is party, or to take steps at	transparent manner in relation to the data subject. **Article 6** sets out specific bases for processing, one of which must apply if processing is to be lawful. Lawful bases include consent of the data subject, necessary for performance of a contract to which the data subject is party, necessary	contrary to the purposes and principles of the Charter of the United Nations.	when the processing is necessary: - to comply with a legal obligation - for implementation of a public interest mission or relevant to the exercise of public authority vested in the controller - for performance of a contract to which the data subject is party or for the application of pre-contractual measures at their request

	or the performance of a legal relationship between the responsible person and the data subject, or for complying with an obligation imposed on the responsible person by the applicable national legislation, or is carried out by a public authority where necessary for the legitimate exercise of its powers.					- necessary for vital interests - necessary for public interest reasons established or provided by law - necessary for the legitimate interests of the person responsible or third party. Also **14. Lawfulness principle** – strict adherence to internal State law, international law, individual rights and	the request of the data subject prior to entering into a contract - protect the vital interests or fundamental rights and freedoms of the data subject.	for legal obligation to which the controller is subject, necessary to protect vital interests, necessary for tasks carried out in the public interest or in the exercise of official authority, necessary for the purposes of legitimate interests.		- for safeguarding the interests or rights and fundamental liberties of the data subject. Article 24: Principle of legality and fairness – the collection, recording, processing, storage, and transmission of personal data must be carried out in a legal, fair and non-fraudulent manner.

						freedoms. Public authorities' treatment of personal data is subject to powers granted to them by law.				
Principles: **Purpose specification**	**Purpose specification principle** – Personal data should be limited to the fulfilment of the specific, explicit and legitimate purposes of the responsible person; no processing that is non-compatible with the purposes for which personal data was collected,	**Purpose specification principle** – specified … and limited to the fulfilment of those purposes ... or such others as are not incompatible with those purposes.	**Uses of personal information principle** – used only to fulfil the purposes of collection and other compatible or related purposes except with consent, where necessary to provide a requested service or product, by the authority of law.	**Article 5: Quality of data** – Personal data (…) shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.	**Article 5: Legitimacy of data processing and quality of data** – Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed	**17: Purpose principle** – defined, explicit and legitimate purposes.	**Article 13, Principle 3: Principle of purpose, relevance, and storage of processed personal data** – data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible	**Article 5(1)(b):** **Purpose limitation principle** – collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	**Principle of the purpose specification** – The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention	**Article 25: Principle of purpose, relevance and preservation** – Personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes.

	unless unambiguous consent of the data subject is given. **Principle of Legitimacy:** Personal data can be processed a. after obtaining the free, unambiguous and informed consent of the data subject; b. where a legitimate interest of the responsible person justifies the processing and the legitimate interests, rights and freedoms of data subjects				in a way incompatible with those purposes.		with those purposes.		of the person concerned, in order to make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;	

	do not prevail.								(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.	
Principles: **Proportionality**	**Proportion-ality principle** – Personal data processing should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes so specified.	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where	**Collection limitation principle** – Collection should be limited to information relevant to the purposes.	**Article 5 – Quality of data** Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes	**Article 5: Legitimacy of data processing and quality of data** – Data processing shall be proportionate in relation to the legitimate purposes pursued	**18. Proportionality principle** – The person responsible shall only treat personal data that is appropriate, pertinent and limited to the minimum necessary for the purpose.	**Article 13, Principle 3: Principle of purpose, relevance, and storage of processed personal data** – data collection shall be adequate, relevant and not excessive in relation to the purposes for which	**Article 5(1)(c):** **Data minimisation principle –** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes	**Principle of the purpose specification** – The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a	**Article 25: Principle of purpose, relevance and preservation** – Personal data...shall be adequate and relevant in relation to the purposes for which it is collected and further processed.

	Processed personal data limited to the minimum necessary.	appropriate, with the knowledge or consent of the data subject. Personal data should be relevant to the purposes for which they are to be used.		for which they are stored.	and reflect at all stages a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. Personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which		they are collected and further processed.	for which they are processed.	certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified.	

					they are processed.					
Principles: **Data quality**	**Data Quality Principle –** The responsible person should at all times ensure that personal data are accurate, sufficient and kept up-to-date to fulfil the purposes for which they are processed. Retention period of processed personal data limited to the minimum necessary, when personal data are no longer necessary to fulfil the purposes	8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	**Integrity of personal information principle** – Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes.	**Article 5: Quality of data** – Personal data (…) shall be accurate and, where necessary, kept up to date and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.	**Article 5: Legitimacy of data processing and quality of data** – Personal data undergoing processing shall be accurate and, where necessary, kept up to date and preserved in a form which permits identification of data subjects for no longer than is	**19. Quality principle** – The person responsible shall adopt necessary measures to keep personal data accurate, complete and updated.	**Article 12, Principle 4: Principle of accuracy of personal data** – data collected shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected/ further processed,	**Article 5(1)(d):** **Accuracy principle** – Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified	**Principle of accuracy** - Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up	**Article 28: Principle of accuracy** – Personal data obtained shall be accurate and, where necessary, kept up to date. All reasonable measures shall be undertaken to ensure that data that is inaccurate and incomplete in relation to the purposes for which it is obtained and further processed shall be erased or rectified.

	which legitimized their processing they must be deleted or rendered anonymous.				necessary for the purposes for which those data are processed.		are erased or rectified.	without delay.	to date regularly or when the information contained in a file is used, as long as they are being processed.	
Principles: **Openness / transparency** **+ Exemptions where applicable**	**Openness principle –** The responsible person shall have transparent policies with regard to the processing of personal data. The responsible person to provide to the data subject information about the responsible person's	12. There should be a general policy of openness about develop-ments, practices and policies with respect to personal data. Means should be readily available of establish-	**Notice principle** – clear and easily accessible statements should be provided about practices and policies **Exemptions:** - collection and use of publicly available inform-ation, - collection and use of	**Article 8 – Additional safeguards for the data subject** Any person shall be enabled: to establish the existence of an automated personal data file, its main purposes, as well as the identity and	**Article 5: Legitimacy of data processing and quality of data** – Personal data under-going processing shall be processed fairly and in a transpare nt manner	**16. Transparency principle** – The person responsible shall inform the holder about the existence and main characteristics of the treatment of personal data (identity, purposes, recipients, rights, origin of data).	**Article 13, Principle 5: Principle of transparency of personal data processing** – requires mandatory disclosure of information on personal data by the data controller. **Article 16: Right to information** – the data	**Article 5(1)(a): Lawfulness, fairness and transparency principle –** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.	**Principle of the purpose specification** – The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to	**Article 27: Principle of transparency** – implies that the data controller is obliged to provide information about the processing of the data. **Article 38: Right to information** – the data controller shall provide the individual

	identity, the intended purpose of processing, the recipients to whom their personal data will be disclosed and how data subjects may exercise these rights and further information necessary to guarantee fair processing of such data. When personal data have been collected directly from the data subject, the information must be provided at the time of collection,	ing 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.	information identifying an individual in their professional capacity.	habitual residence or principal place of business of the controller of the file.	**Article 8: Transparency of processing** – controller to inform data subjects of identity, habitual residence or establishment; legal basis and purposes of processing, the categories of personal data processed, recipients, or categories of recipients, the means of		controller shall provide the natural person whose data are to be processed with information on its identity, purposes, categories of data, recipients, existence of certain rights, storage period, and proposed transfers to third countries.		the attention of the person concerned.	whose personal data is being processed with information on its identity, purposes, recipients, existence of certain rights, the preservation period, and possibility of transfer to a third country.

	unless already provided. When personal data have not been collected directly from the data subject, the responsible person must also inform him/her about the source of personal data, within a reasonable period of time but may be replaced by alternative measures if compliance is impossible or would involve a disproportionate effort by the				exercising data subject's rights **Exemption** **Article 11: Exceptions and restrictions** – when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate					

	responsible person. Any information to be furnished to the data subject in an intelligible form, using clear and plain language, in particular for any processing addressed specifically to minors. When personal data is collected online, by means of electronic communications networks, the obligations set out above may be				measure in a democratic society for: - protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of					

	satisfied by posting privacy policies, easy to access and identify, and which include all the information mentioned above.				criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. Restrictions may be provided					

					for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.					

Principles: **Accountability**	**Accountability principle** – The responsible person shall take all necessary measures to observe the principles and obligations set out in this Resolution and in the applicable national legislation and have the necessary internal mechanism in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise	14. A data controller should be account-able for complying with measures which give effect to the principles stated above. 15. A data controller should: a) Have in place a privacy management programme and be prepared to demon-strate the prog-ramme as appropriate, in	**Accountability principle** – controller should be account-able for complying with measures that give effect to the principles. When inform-ation is transferred to another, the controller should obtain consent or exercise due diligence, taking reasonable steps to ensure that the recipient will protect the		**Article 10: Additional obligations** – each Party shall provide that Contr-ollers and, where applicable, processors, take all appropriate measures to comply with the obligat-ions of this Convent-ion and be able to demon-strate that the data processing under their control is in	**20. Responsibility principle** – The person responsible shall implement necessary mechanisms to prove compliance, shall be accountable to the holder and to the control authority. Mechanisms to adopt may be: - data protection programs and policies - risk management systems - training		**Article 5(2): Accountability principle** – The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the principles] **Article 24: Responsibility of the controller** - The controller shall implement appropriate technical and organisational measures to ensure		

	of their powers as established under section on Compliance and monitoring: Independent Supervisory authorities powers and competences.	particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines.	information in line with the principles.		compliance.	- reviews of policies and programs - audits - complaints procedures.		and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.		
Principles: Security	Both the responsible person and any processing service	11. Personal data should be protected by	**Security Safeguards principle** – appropriate safeguards against	**Article 7: Data security** – Appropriate security measures	**Article 7: Data security** – Each party shall provide	**21. Safety principle** – The person responsible shall establish and	**Article 13, Principle 6: Principle of confidentiality and security of**	**Article 5(1)(f): Integrity and confidentiality principle**	**Principle of security** – Appropriate measures should be taken to	**Article 28: Principle of confidentiality and security –** Personal data shall be

	provider must protect the personal data subject to processing with the appropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability.	reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	loss/ unauthorised access; unauthorised destruction, use, modification, disclosure.	shall be taken for the protection of personal data stored in automated data files against accidental or unauth-orised destruction or accidental loss as well as against unauth-orised access, alteration or dissem-ination.	that the controller, and where applicable the processor, takes appropriate security measures against risks such as accidental or unauth-orised access to, dest-ruction, loss, use, modif-ication or disclosure of personal data.	maintain sufficient administrative, physical and technical measures in order to guarantee the confident-iality, integrity and availability of personal data.	**personal data processing** – personal data shall be processed confidentially and protected, in particular where the processing involved transmission of the data over a network. Controllers and processors must ensure compliance with security measures defined in this Convention. **Article 21: Security obligations** – the data	– Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.	processed confidentially and shall be protected, in particular when processing includes transmission of data on a network. **Article 43: Obligations of security** – the data controller shall take all necessary precautions in relation to the nature of data, and in particular to ensure that it is not deformed, damaged or accessible to

							controller must take all appropriate precautions, according to the nature of the data, and in particular, to prevent such data from being altered or destroyed, or accessed by unauthorized third parties.	**Article 32: Security of processing –** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement		unauthorised third parties.

								appropriate technical and organisational measures to ensure a level of security appropriate to the risk.		
Principles : Data retention	**Data quality principle:** the responsible person shall limit the period of retention of the processed personal data to the minimum necessary. When personal data are no longer necessary to fulfil the purposes they must be deleted or			**Article 5: Quality of data** – Personal data shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which	**Article 5: Legitimacy of data processing and quality of data** – Personal data undergoing processing shall be preserved in a form which permits identification of data subjects	**19. Quality principle** – When personal data is no longer necessary for the purpose, the person responsible shall delete or remove it from its archives, records, databases, files, systems, or anonymize it.	**Article 13,** **Principle 3: Principle of purpose, relevance, and storage of processed personal data** – data shall be kept for no longer than is necessary for the purposes for which the data were collected or further processed.	**Article 5(1)(e): Storage limitation principle** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the	**Principle of the purpose specification** – The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or	**Article 25: Principle of purpose, relevance and preservation** – Personal data…shall be kept for a period which shall not exceed the period required for the purposes for which they were obtained and processed. Beyond the required

	rendered anonymous.			those data are stored.	for no longer than is necessary for the purposes for which those data are processed.		Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law. **Article 22: Storage obligations** – personal data shall be kept no longer than is necessary for the purposes for which the data were collected or processed.	personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical	be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.	period, data may only be kept with a view to responding specifically to processing for historical, statistical and research purposes, in line with existing legal provisions. **Article 44: Obligations of preservation** – Personal data shall be kept for a period of time set by a regulatory text and only for the purposes for which they were obtained.

								and organisatio nal measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.		
Data subject rights										
Data subject rights: **Access** **+ Exemptions**	**Right of access –** Data subject has the right upon request to obtain information on the specific personal data	13. Individuals should have the right: a) to obtain from a data controller,	**Access and Correction principle** – individuals should be able to obtain confirmatio n of processing and to have the	**Article 8: Additional safeguards for the data subject** – Any person shall be enabled to obtain (…) confirmatio n of	**Article 9: Rights of the data subject** – Every individual shall have the right to obtain, on request (…)	**25. Right to Access** – Holder shall have the right to request access to its personal data in possession of the	**Article 17: Right of access** – Natural persons whose data are to be processed can request information to enable	**Article 15: Right of access by the data subject –** The data subject shall have the right to obtain from the	**Principle of interested person access** – Everyone who offers proof of identity has the right to know whether	**Article 39: Right of access** – an individual whose personal data is the subject of processing may request information to enable them

	subject to processing, as well as the source of such data, the purposes of processing and the recipients or categories of recipients to whom such data are or will be disclosed. Information to the data subject must be provided in an intelligible form, clear and simple language. The responsible person must implement procedures to enable this right to be exercised in a	or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonabl	information communicated to them **Exemptions:** - unreasonable or disproportionate burden or expense - legal or security reasons, or commercial confidentiality - violation of other individuals' information privacy.	whether personal data are stored as well as communication to him of such data in an intelligible form. **Exemptions** **Article 9:** - when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:	confirmation of the processing, communication in an intelligible form of the data processed. **Exceptions, restrictions:** **Exemptions:** **Article 11: Exceptions and restrictions** – when such an exception is provided for by law, respects the essence of	responsible person. **Exemptions:** National legislation shall establish, but could be: - treatment necessary for compliance with an important purpose of public interest - treatment necessary for exercising the functions of public authorities - person responsible's legitimate motives prevail over holder's	them to evaluate the processing, confirmation as to whether data are being processed, the data being processed and any information as to its source, the purpose of processing and recipients.	controller confirmation as to whether or not personal data concerning him or her are being processed, access to the personal data and information about purposes of the processing; categories of personal data; recipients or categories of recipient; retention period or criteria used to determine	information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if	to be informed of and contest the processing, confirmation as to whether data are being processed, disclosure of the data being processed and any information as to its origin, the purpose of processing and recipients.

	simple, fast and efficient way, with not undue delay or cost of gain for the responsible person. The data subject must be informed of the reasons, if the exercise of this right under applicable national legislations is not justified. **Exemptions:** National legislation may limit repetitive exercise of this right when responding to multiple	e manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge		- protecting state security; public safety; monetary interests of state or the suppression of criminal offences - protecting the data subject and the rights and freedoms of others - Restrictions may be provided by law with respect to data used for statistics or scientific research purposes and where there is	the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: - protection of national security, defence, public safety, important economic and financial interests of the State, the	interests, rights and freedoms - treatment necessary for compliance with a legal obligation - personal data necessary for maintenance or compliance with a legal or contractual relation.		it; the existence of other data subject rights; information as to the source of the data; the existence of automated decision-making, including profiling, and information about the logic involved; if data is transferred to a third country or international organisation, information about safeguards;	need be with the supervisory authority specified in principle 8. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence. **Exemptions:** Exceptions authorized only as necessary to protect national security, public order, public health or morality, as well as, inter alia, the	

	requests within a short time period, unless the data subject states a legitimate reason when exercising this right.	is successful to have the data erased, rectified, completed or amended.		obviously no risk of an infringement of the privacy of the data subjects.	impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights and fundamen			and a copy of the personal data undergoing processing. **Exemptions:** Where providing access adversely affects the rights and freedoms of others.	rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.	

					tal freedoms of others, notably freedom of expression. Restrictions may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where					

					there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.					
Data subject rights: **Objection / opposition** **+ Exemptions**	**Right to object:** The data subject may object to personal data processing where there is a legitimate reason related to his/her specific personal situation. This right may be exercised directly by the			To an extent: **Article 8 – Additional safeguards for the data subject** Any person shall be enabled: to obtain (…) erasure of such data if these have been processed contrary to the	**Article 9: Rights of the data subject** – Every individual shall have a right to object at any time (…) to the processing of personal data concerning him or her unless the	**28. Right to Opposition** – Holder may oppose the treatment of its personal data when: - it has a legitimate reason in the particular situation - the purpose of the treatment is direct marketing,	**Article 18: Right to object** – natural person has the right to object, on legitimate grounds, to processing relating to him/her. They also have the right to be informed before personal data	**Article 21:** **Right to object –** The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of their personal data based		**Article 40: Right to object** – an individual is entitled, for legitimate reasons, to object to processing of personal data of which he is the data subject. They are also entitled to be informed before personal data

	data subject, satisfactorily establishing his/her identity, or through a representative, satisfactorily establishing his/her identity. The responsible person must implement procedures to enable this right to be exercised in a simple, fast and efficient way, with not undue delay or cost of gain for the responsible person. The data subject must be informed of			provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention.	controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms. **Exemptions:** **Article 11: Exceptions and restrictions** – when such an exception is provided for by law, respects	including profiling. **Exemptions:** National legislation shall establish, but could be: - treatment necessary for compliance with an important purpose of public interest - treatment necessary for exercising the functions of public authorities - the person responsible's legitimate motives prevail over holder's	relating to them is disclosed for the first time to third parties, or used for marketing, and to be offered the right to object to those disclosures/ uses.	on certain lawful bases. The right to object applies at any time when processing is for the purposes of direct marketing.		relating to them is disclosed for the first time to third parties, or used on behalf of a third party for marketing, and to be offered the right to object to those disclosures/ uses.

	the reasons, if the exercise of this right under applicable national legislations is not justified. **Exemptions:** The exercise of this right is not justified where the processing is necessary for the performance of a duty imposed on the responsible person by the applicable national legislation. The data subject may also object to those				the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: - protection of national security, defence, public safety, important economic and financial interests	interests, rights and freedoms - treatment necessary for compliance with a legal obligation - personal data necessary for maintenance or compliance with a legal or contractual relation.				

	decisions which produce legal effects based solely on automated processing except when the decision has been specifically requested by the data subject or necessary for the establishment, maintenance or performance of a legal relation between the responsible person and the data subject – in the latter case, the data subject must put forward his/her				of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights					

	viewpoint in order to defend his/her right/interest.				and fundamental freedoms of others, notably freedom of expression. Restrictions may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical					

					purposes where there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.					
Data subject rights: **Rectification** **+ Exemptions**	**Rights to rectify –** The data subject has the right to request from the responsible person the rectification of personal data that is incomplete, inaccurate, unnecessary or excessive. Where justified, the	13. Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller	**Access and Correction principle** – individuals should be able to challenge the accuracy of personal information, and if possible and as appropriate have the information rectified, completed,	**Article 8: Additional safeguards for the data subject** – Any person shall be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to	**Article 9: Rights of the data subject** – Every individual shall have a right to obtain, on request (…) rectification or erasure, as the case may be, of such data	**26. Right to Correction** – Holder shall have the right to obtain from the person responsible the correction of its personal data when they are inaccurate, incomplete or are not updated.	**Article 19: Right of rectification or erasure** – Any natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, personal data concerning him/her	**Article 16: Right to rectification** – The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data	**Principle of interested person access** – Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible	**Article 41: Right to rectification and destruction** – if personal data are inaccurate, incomplete, questionable, outdated or prohibited from collection, use, disclosure or preservation, the data

	responsible person should carry out the rectification and notify third parties to whom personal data has been disclosed, if known. The responsible person must implement procedures to enable this right to be exercised in a simple, fast and efficient way, with not undue delay or cost of gain for the responsible person. The data subject must be informed of the reasons, If	has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given	amended or deleted. **Exemptions:** - unreasonable or disproportionate burden or expense - legal or security reasons, or commercial confidentiality - violation of other individuals' information privacy.	the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 (Quality of data, special categories of data) **Exceptions and restrictions:** **Article 9:** - when such derogation is provided for by the law of the Party and constitutes a necessary measure in a	if these are being, or have been, processed contrary to the provisions of this Convention. **Exceptions and restrictions:** **Article 11: Exceptions and restrictions** – when such an exception is provided for by law, respects the essence of the	**Exemptions:** National legislation shall establish, but could be: - treatment necessary for compliance with an important purpose of public interest - treatment necessary for exercising the functions of public authorities - the person responsible's legitimate motives prevail over holder's interests,	where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited.	concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **Article 19: Notification obligation –** controller shall communicate any rectification or erasure	form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8. The cost of	subject is entitled to ask the controller to have the data rectified, supplemented, updated, blocked or destroyed as appropriate.

	the exercise of this right under applicable national legislations is not justified.	reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.		democratic society in the interests of: - protecting state security; public safety; monetary interests of state or the suppression of criminal offences - protecting the data subject and the rights and freedoms of others - Restrictions may be provided by law with respect to data used for statistics	fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: - protection of national security, defence, public safety, important economic and financial interests of the State, the impartialit	rights and freedoms - treatment necessary for compliance with a legal obligation - personal data necessary for maintenance or compliance with a legal or contractual relation.		of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.	any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence. **Exemptions:** Exceptions authorized only as necessary to protect national security, public order, public health or morality, as well as,	

				or scientific research purposes and where there is obviously no risk of an infringement of the privacy of the data subjects.	y and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights and fundamental				inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.	

					freedoms of others, notably freedom of expression. Restrictions may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where there is no					

					recognisable risk of infringement of the rights and fundamental freedoms of data subjects.					
Data subject rights: **Deletion / erasure (including right to be delisted)** **+ Exemptions**	**Right to delete –** The data subject has the right to deletion of personal data that is incomplete, inaccurate, unnecessary or excessive. Where justified, third parties to whom that personal data has been disclosed	13. Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data	**Access and Correction principle** – individuals should be able to challenge the accuracy of personal information, and if possible and as appropriate have the information rectified, completed, amended or deleted.	**Article 8: Additional safeguards for the data subject** – Any person shall be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions	**Article 9: Rights of the data subject** – Every individual shall have a right to obtain, on request.. rectification or erasure, as the case may be, of such data if these are being, or have	**27. Right to cancellation** – Holder shall have the right to request the cancellation or removal of its personal data from the archives, records, files and systems of the person responsible, in order for them not to be in its possession and for the	**Article 19: Right of rectification or erasure** – Any natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, personal data concerning him/her where such data are	**Article 17 Right to erasure ('right to be forgotten') –** The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and	**Principle of interested person access** – Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without	**Article 41: Right to rectification and destruction** – if personal data are inaccurate, incomplete, questionable, outdated or prohibited from collection, use, disclosure or preservation, the data subject is entitled to ask

	should also be notified, where known. The responsible person must implement procedures to enable this right to be exercised in a simple, fast and efficient way, with not undue delay or cost of gain for the responsible person. The data subject must be informed of the reasons, if the exercise of this right under applicable national legislations is not justified.	relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if	**Exemptions:** - unreasonable or disproportionate burden or expense - legal or security reasons, or commercial confidentiality - violation of other individuals' information privacy.	of domestic law giving effect to the basic principles set out in Articles 5 and 6 (Quality of data, special categories of data) **Exceptions and restrictions:** **Article 9:** - when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in	been, processed contrary to the provisions of this Convention. **Exceptions and restrictions:** **Article 11: Exceptions and restrictions** – when such an exception is provided for by law, respects the essence of the fundamental rights and	person responsible to stop treating them. **Exemptions:** National legislation shall establish, but could be: - treatment necessary for compliance with an important purpose of public interest - treatment necessary for exercising the functions of public authorities - person responsible's legitimate	inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited.	the controller shall have the obligation to erase personal data without undue delay where certain grounds apply. **Article 19: Notification obligation** - controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the	undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8. It is desirable that the provisions of	the controller to have the data rectified, supplemented, updated, blocked or destroyed as appropriate.

	Exemptions: Deletion of personal data is not justified where personal data must be retained for performance of an obligation imposed on the responsible person by the applicable national legislation, or by contractual relations between the responsible person and the data subject.	a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.		the interests of: - protecting state security; public safety; monetary interests of state or the suppression of criminal offences - protecting the data subject and the rights and freedoms of others - Restrictions may be provided by law with respect to data used for statistics or scientific research	freedoms and constitutes a necessary and proportionate measure in a democratic society for: - protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the	motives prevail over holder's interests, rights and freedoms - treatment necessary for compliance with a legal obligation - personal data necessary for maintenance or compliance with a legal or contractual relation.		personal data have been disclosed, unless this proves impossible or involves disproportionate effort.	this principle should apply to everyone, irrespective of nationality or place of residence. **Exemptions:** Exceptions authorized only as necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause)	

				purposes and where there is obviously no risk of an infringement of the privacy of the data subjects.	judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the protection of the data subject or the rights and fundamental freedoms of others, notably				provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.	

					freedom of expression. Restrictions may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where there is no recognisable risk of infringem					

					ent of the rights and fundamental freedoms of data subjects.					
Data subject rights: **Right to restriction of processing** **+ Exemptions**						**31. Right to the Limitation of treatment of Personal Data** – Holder shall have the right to have the treatment of its personal data limited to its storage during the period of time between a rectification or opposition request, until its resolution by the		**Article 18: Right to restriction of processing –** The data subject shall have the right to obtain from the controller restriction of processing where the data subject contests its accuracy, the processing is unlawful, the		

						person responsible.		controller no longer needs the data but it is required by the data subject for legal claims, or the data subject has objected to the processing pending decision. **Article 19: Notification obligation** - controller shall communica te any rectification or erasure of personal data or restriction of processing to each recipient to		

								whom the personal data have been disclosed, unless this proves impossible or involves disproporti onate effort.		
Data subject rights: **Portability** **+ Exemptions**						**30.Right to Portability of Personal Data** – Holder has the right to obtain a copy of personal data provided (telephone or automated) in a structured electronic format, that allows them to use or transfer to		**Article 20: Right to data portability** – The data subject shall have the right to receive their personal data which they have provided to a controller, in a structured, commonly used and		

						another person responsible. Can request data to be transferred directly when technically possible. **Exemptions:** National legislation shall establish, but could be: - treatment necessary for compliance with an important purpose of public interest - treatment necessary for exercising the functions		machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or contract and is automated.		

						of public authorities - person responsible's legitimate motives prevail over holder's interests, rights and freedoms - treatment necessary for compliance with a legal obligation - personal data necessary for maintenance or compliance with a legal or contractual relation.				
Data subject rights:					**Article 9: Rights of the data subject** –	**29. Right not to be subject to Automated**		**Article 22: Automated individual decision-**		**Article 35: Basis of a Court decision** – Art 35, 1: No

Automated decisions **+ Exemptions**					Every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration **Exemption** If the decision is authorised	**Individual Decision**s – Holder shall have the right not to be the subject of decisions causing significant/ legal effects, based only on automated treatments assessing, analysing or predicting professional performance, economic situation, health status, sexual preference, reliability, or behaviour. **Exemption**		**making, including profiling** – The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or other similar effects, unless the decision is necessary for entering into, or performance of, a contract between the data		court decision implying an assessment of the behaviour of an individual shall be based on the processing by automatic means of personal data for the purpose of evaluating certain aspects of their personality. Art 35, 2: no decision that has legal effect on an individual shall be based solely on processing by automatic means of personal data for the

					by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. **Exceptions and restrictions:** **Article 11: Exceptions and restrictions** – when such an	- necessary for the execution of an agreement between the holder and the person responsible - holder consent Though in either case the holder has the right to obtain human intervention, receive an explanation, and appeal the decision.		subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable safeguards; or is based on the data subject's explicit consent. The data controller shall implement suitable safeguards, at least the right to obtain human interventio		purpose of defining the profile of the subject or evaluating certain aspects of their personality.

					exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: - protection of national security, defence, public safety,			n on the part of the controller, to express his or her point of view and to contest the decision. Further limitations apply where decisions are based on special categories of personal data.		

					important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; and the					

					protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. Restrictions may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or					

					historical research purposes or statistical purposes where there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.					
Accountability standards										
Accountability standards: **Data protection officer**	The appointment of one or more data protection or privacy officers, with				**Article 9.1** 1. Each Party shall provide that	**39. Official Protection of Personal Data** – The person responsible shall appoint		**Articles 37, 38, 39: Data protection officer** – Controllers and processors		

	adequate qualifications, resources and powers for exercising their supervisory functions adequately. The responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical, organizational measures to ensure each time, their integrity, confidentiality and availability.				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 compliance with the provisions of this Convention.	a personal data protection officer when: - it is a public authority - purpose of treatment is the regular or systematic observation of holder's conduct - performs treatments where a high risk to the data protection rights of holders is likely - if none of the above apply, a data protection officer can still be appointed.		must designate a data protection officer in certain cases, and their position and tasks are specified.		

	Dependent on existing risk, possible consequences to the data subjects, sensitivity of personal data, the context of processing and obligations as set out in national legislation.				**Explanatory Report Article 87:** A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a "data protection officer" entrusted with the means necessary to fulfil his or her mandate. Such a					

					data protection officer, whose desig-nation should be notified to the super-visory authority, could be internal or external to the controller.					
Accountability standards: **Breach prevention, response plans and reporting measures**	Data Subjects should be informed by those involved in any stage of the processing of any security breach that could significantly affect their pecuniary or non-	15. A data controller should: a) Have in place a privacy management programme that: i. gives effect to these Guidelines	Member economies should consider encouraging controllers to develop and implement Privacy Management Programmes, which should provide		**Article 7.2:** Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority	**22. Notice of Violation to the Safety of Personal Data** – The person responsible must notify the holder and the control authority if they become aware of damage, loss,		**Article 33 Notification of a personal data breach to the supervisory authority** – must be reported within 72 hours unless the breach is unlikely to		

	pecuniary rights, as well as measures taken for resolution. Information should be provided in good time to enable data subjects to see protection of their rights. States should encourage through their domestic law, implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the	for all personal data under its control; 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	appropriate safeguards, establish internal oversight mechanisms and responses to incidents. Member economies should consider encouraging or requiring controllers to provide notice to PEAs in the event of a significant security breach.		(…) of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.	illegal or unauthorized alteration, destruction or access, unless the violation does not pose a risk to the holder's rights and freedoms.		result in a risk to the rights and freedoms of data subjects. **Article 34: Communication of a personal data breach to the data subject** – controller must inform the data subject if a breach is likely to result in a high risk to their rights and freedoms.		

	protection of privacy with regarding to the processing of personal data: The implementation of procedures to prevent and detect breaches, which may be based on standardized models of information security governance and/or management. The implementation of a response plan that establishes guidelines for action in case of verifying a	governance structure and establishes internal oversight mechanisms; v. includes plans for responding to inquiries and incidents; vi. is updated in light of ongoing monitoring and periodic assessment; b) Be prepared to demonstrate its								

	breach of applicable laws on the protection of privacy with regard to the processing of personal data, including at least the obligation to determine the cause and extent of the breach, to describe its harmful effects and to take the appropriate measures to avoid future breaches.	privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these								

		Guidelines ; 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.								
Accountability standards: **Training**	The periodic implementation of training, education and awareness programs among the members of the organization aimed at better understanding of the appliable laws on the protection of privacy with regard to the processing of personal data, as well as the procedures established by the organization				**Explanatory Report Article 85:** According to article 10 paragraph 1, the obligation on the controller to ensure adequate data protection is linked to the responsibility to verify and be in a position to demonstrate that data processing is in	**20. Responsibility principle** – training noted as a mechanism to adopt to comply with this principle.		**Article 24: Responsibility of the controller** The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those		

	for that purpose.				compliance with the applicable law. The data protection principles set out in the Convention, which are to be applied at all stages of processing, including the design phase, aim at protecting data subjects and are also a mechanism for enhancing their trust. Appropriate measures			measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures referred to shall include the implementation of appropriate data protection policies by the controller.		

					that the controller and processor may have to take to ensure compliance include: training employees; setting up appropriate notification procedures (for instance to indicate when data have to be deleted from the system); establishing specific contractual provisions where the					

					processing is delegated in order to give effect to the Conv-ention; as well as setting up internal procedures to enable the verific-ation and demon-stration of comp-liance.					
Accountability standards: **Audits**	The periodic conduct of transparent audits by qualified and preferably independent parties to verify compliance with the				**Explanatory Report Article 85:** According to article 10 paragraph 1, the obligation on the controller	**20. Responsibility principle** – internal and/or external supervision and surveillance systems, including		**Article 24: Responsibility of the controller** – The controller shall implement appropriate technical and		

	applicable laws on the protection of privacy with regard to the processing of personal data, as well as with the procedures established by the organization for that purpose.				to ensure adequate data protection is linked to the responsibility to verify and be in a position to demonstrate that data processing is in compliance with the applicable law. The data protection principles set out in the Convention, which are to be applied at all stages of processing	audits, noted as a mechanism to adopt to comply with this principle.		organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures referred to		

					, including the design phase, aim at protecting data subjects and are also a mechanism for enhancing their trust. Appropriate measures that the controller and processor may have to take to ensure compliance include: training employees; setting up appropriate notific-			shall include the implementation of appropriate data protection policies by the controller.		

					ation proced-ures (for instance to indicate when data have to be deleted from the system); establish-ing specific contract-ual provisions where the processing is delegated in order to give effect to the Convent-ion; as well as setting up internal proced-ures to enable the verific-					

					ation and demon-stration of comp-liance.					
Accountability standards: **Privacy by design**	The adaptation of information systems and/or technologies for the processing of personal data to the 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 development and		Promotion of technical measures to protect privacy. Member economies should promote technical measures which help to protect privacy. Member economies may encourage controllers to make full use of readily available technical safeguards and measures, and may also		**Article 10: Additional oblig-ations** – Each Party shall provide that controllers and, where applicable, processors (…) shall design the data processing in such a manner as to prevent or minimise the risk of interf-erence with those	**38. Privacy Due to Design and Privacy by Default** – The person responsible shall apply preventive measures from the design stage. The person responsible shall guarantee that its programs, services, computing systems, applications or other technology that treats personal		**Article 25: 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 purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of		

	implementation thereof.		support the development of technical standards that embed best privacy practice into systems engineering.		rights and fundamental freedoms.	data, comply by default or adapt to the principles, rights, and other obligations provided by the applicable national legislation.		natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data		

								protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational		

								measures 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 not making personal data by default accessible to an indefinite number of persons. An approved certification mechanism could assist in demonstrating the above.		
Accountability standards: **Impact assessments**	The implementation of privacy impact assessments prior to implementing new information systems and/or technologies				**Article 10: Additional obligation** – Each party shall provide that controllers and, where applicable, processors	**41. Impact Assessment on the Protection of Personal Data** – The person responsible shall perform an impact assessment prior to		**Section 3: Data protection impact assessment and prior consultation** **Article 35: Data protection**		

	for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing.				, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing.	implementation of treatment of personal data that probably entails a data protection high risk. National legislation shall set out the treatments that will require an impact assessment; its contents; and the requirements around submission to the control authority.		**impact assessment** – Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the 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 of personal data. **Article 36: Prior consult-ation** – The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing		

								would result in a high risk in the absence of measures taken by the controller to mitigate the risk.		
Account-ability standards: **Codes of conduct/ practice; certificatio n schemes**	The adoption of codes of practice the observance of which are binding and that include elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in				**Explanato ry Report Article 127:** In addition to this consultati on foreseen under paragraph 3, the authority could also be asked to give its opinion when other measures concernin	**40. Self-regulation Mechanisms** – Codes of ethics and certification systems (and other systems) can be developed, validated by rules established in national legislation. The person responsible may voluntarily adhere to		**Section 5: Codes of conduct and certif-ication** **Article 40: Codes of conduct** – Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct by Associat-		

	case of non-compliance. The responsible person and those involved in processing shall maintain confidentiality of personal data. This obligation shall remain even after the ending of the relationship with the data subject, or with responsible person.				g personal data processing are in prepar-ation, such as for instance codes of conduct or technical norms.	those schemes, whose purpose is the correct application of the law, to establish conflict resolution between the person responsible and the holder.		ions and other bodies, intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprise. **Article 41 Monitoring of approved codes of conduct –** Codes will		

								be monitored by a body accredited by the competent supervisory authority. A**rticle 42: Certific-ation** – Member States, the supervisory authorities, the Board and the Commission shall encourage the establishment of data protection certification mechanism and of data protection seals and marks, for the purpose		

								of demonstrating compliance. **Article 43: Certification bodies** – Certification bodies will be accredited.		
Accountability standards: **Records of processing activities**	Implied by accountability requirements.	Implied by accountability requirements.			Implied by accountability requirements.	Implied by accountability requirements.		**Article 30: Records of processing activities** – Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. Article 30 lists		

								what the record must contain.		
Specific themes/ requirements: **Sensitive data**	**Sensitive Data –** Personal data which affect the data subject's most intimate sphere or data likely to give rise, in case of misuse, to unlawful or arbitrary discrimination or a serious risk to the data subject. In particular personal data revealing racial or ethnic origin, political opinions, religious or			**Article 6: Special categories of data** – Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate	**Article 6: Special categories of data** – Processing of genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data; personal data for the information they reveal	**9. Treatment of Sensitive Personal Data** – (Racial or ethnic origin, beliefs or religious, philosophical or moral convictions, union affiliation, political opinions, information regarding health, life, sexual preference or orientations, generic [genetic?] data or biometric data) may not be	**Article 14: Specific principles for the processing of sensitive data** – State Parties shall undertake to prohibit processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information,	**Article 9 Processing of special categories of personal data –** Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of	**Principle of non-discrimination** – Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as	**Article 30: Specific principles** – it is prohibited to obtain and process data that reveals the racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sexual life, genetic data or health data. **Article 31: Exceptions** – contains a number of

	philosophical beliefs, as well as health, sex life. Other categories of sensitive data may apply as applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.			safeguards. The same shall apply to personal data relating to criminal convictions	relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law complementing those of this Convention.	treated unless: - strictly necessary for exercise/ compliance with powers and obligations in rules that regulate their actions - they comply with a legal mandate - the holder consents - necessary for national security, public security, public order, public health, or the safekeeping of the rights and	health data, unless: - data is manifestly made public by the data subject - data subject has given consent - processing necessary to protect the vital interests of the data subject or another person - processing required for legal claims - judicial procedures, criminal investing-ations - necessary in the public interest,	uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited unless one of a number of conditions apply, such as explicit consent, necessary for obligations and rights in employment, social security or social	membership of an association or trade union, should not be compiled.	exceptions to the prohibition in Article 30 – includes: - data manifestly made public by the data subject - written consent of the data subject - necessary to protect vital interests - (in particular genetic data) necessary for legal rights - legal proceedings or criminal investigations - necessary for reasons of public interest, in particular for

						freedoms of third parties.	especially for historical, statistical or scientific purposes - necessary for the performance of a contract - necessary for compliance with a legal or regulatory obligation - necessary for the performance of a task in the public interest/ exercise of official authority - legitimate activities of a non-profit making body with political, philosophical	protection law, necessary for vital interests, necessary for legitimate activities of a not for profit political, philosophical, religious or trade union aim, personal data manifestly made public by the data subject, necessary for legal claims, substantial public interest, necessary for health or public health		historical, statistical or scientific purposes - necessary for performance of a contract and pre-contractual measures - necessary for compliance with a legal or regulatory obligation - necessary for implementation of a public interest mission, or carried out by a public authority or assigned by a public authority - legitimate activities of a non-profit making body

							, religious, cooperative or trade union aim - literary or artistic expression/ journalism, National law with regard to print media or the audio-visual sector still applies. No decisions producing legal or other significant effects based solely on automated processing. No transfers to non-Member States unless an adequate level of protection is	purposes, necessary for archiving in the public interest, historical or scientific research purposes.		for political, philosophical, religious, mutual benefit or trade union purposes.

							in place, or authorized by the national protection authority.			
Specific themes/ requirements: **Processors**	**Provision of processing services –** The responsible person may carry out processing of personal data through one or more processing service providers, without disclosure of data to a third party, provided that: a. the processing provider guarantees the level of protection as specified in				**Explanatory Report** **Article 24** "Processor" is any natural or legal person (other than an employee of the data controller) who processes data on behalf of the controller and according to the controller's instruction	**33. Scope of the Person in Charge** – has no decision power over the scope and contents of the personal data. Limits its acts to the terms established by the person responsible. **34. Formalization of the Provision of Services of the Person in Charge –** By an agreement or other legal instrument,		**Article 28: Processor** – controllers shall only use processors providing sufficient guarantees; processors shall not engage another processor without the authorisation of the controller; processing shall be governed by a contract.		**Article 29: Principle of choice of data processor** – data controllers must choose a data processor providing sufficient guarantees. It is the responsibility of the data controller, as well as the data processor to ensure compliance with the security measures defined in this Supplementary Act.

	this Resolution and applicable national legislation; and b. the legal relationship established through a contract or legal instrument that allows proving its existence, scope and content, and that sets out the processing service provider's obligation to comply with these guarantees and ensure that personal				s. The instructions given by the controller establish the limit of what the processor is allowed to do with the personal data.	which establishes subject, scope, contents, duration, nature and purpose, type of personal data. Certain general clauses must be included in the agreement.				

	data is processed compliance in with instructions from the responsible person.									
Specific themes/ requirements: **Joint controllers**					**Explanatory Report Article 22:** In some cases, there may be multiple controllers or co-controllers (jointly responsible for a processing and possibly responsible for different aspects of that			**Article 26: Joint controllers –** Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their		

					processing).			respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective		

								responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrange-ment may designate a contact point for data subjects.		
Specific themes/ requirements: **Vulnerable or other groups of data subjects, e.g. children**					**Article 15: Supervisory authorities** – authorities shall promote public awareness of their functions,	**8. Treatment of Personal Data of Girls, Boys and Adolescents** – special protection in accordance with the Convention on the Rights of the Child		**Article 8: Conditions applicable to child's consent in relation to information society services** – Where processing is based on		

					powers and activities, of the rights of data subjects and the exercise of such rights, and awareness of controller and processors of their responsibilities under this Convention – specific attention shall be given to the data protection rights of children and other vulnerable	and other international instruments - States shall promote in academic education the responsible, appropriate and safe use of technology and digital risks, and rights and freedoms.		data subject consent, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised		

					individuals.			by the holder of parental responsibility over the child. **Article 12: Transparent information** – Information relating to processing should be communicated in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed		

								specifically to a child.		
Specific themes/ requirements: **professional secrecy and supervisory authority investigations**								**Article 90 Obligations of secrecy –** Member States may adopt specific rules to set out the investigative powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject to an obligation of professional		

								secrecy or other equivalent obligations of secrecy where this is necessary and proportion-ate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of		

								or has obtained in an activity covered by that obligation of secrecy.		
Compliance and monitoring: **Independent supervisory authorities' powers and competences**	**Monitoring** In every State, there shall be one or more supervisory authorities, in accordance with domestic law, that will be responsible for supervising the observance of the principles set out in the Resolution, who shall be impartial and independent, and will have		The APEC Framework can be enforced via various models, as deemed appropriate by the member economy in question. Can include Privacy Enforcement Authorities (PEAs), multi-agency enforcement bodies, networks of designated	**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**	**Article 15: Supervisory authorities** – Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention. Article contains detailed requireme	**42. Nature of Control and Supervision Authorities** – There must be one or more control authorities on personal data protection in each Ibero-American State. Control authorities shall be free of any external influence and shall not request nor admit any	**Article 11: Status, composition and organization of National Personal Data Protection Authorities –** Each State Party shall establish an authority in charge of protecting personal data. It shall be an independent administrative authority with the task	**Article 51: Supervisory authority –** Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation. **Article 55 Competenc**	**Supervision and sanctions** – 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. This authority shall offer	**Article 14: Establishment** – within the ECOWAS space, each Member State shall establish its own data protection Authority. It shall be an independent administrative Authority responsible for ensuring that personal data is processed in compliance with the provisions of the

	technical competence, sufficient powers and adequate resources to deal with claims by data subjects and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy regarding processing personal data. In any case, without prejudice to any administrative		industry bodies, courts and tribunals, or a combination of the above. However, member economies are encouraged to establish PEAs, and those that are established should be provided with the governance, resources and technical expertise necessary to exercise their powers effectively. Economy must	**Article 1 Supervisory authorities** Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol. To this end, the said authorities shall have,	nts, including powers of investigation and intervention; approval of safeguards for transborder data flows; powers to issue decisions and impose administrative sanctions, and to engage in legal proceedings. Authorities shall be consulted on	order or instruction. Applicable national legislation must grant control authorities sufficient investigation, supervision, resolution, promotion, sanction and other powers necessary to guarantee effective compliance. Control authorities must have the necessary human and material resources for complying with their functions.	of ensuring that the processing of personal data complies with the Convention. **Article 12: Duties and Powers of National Protection Authorities –** duties include responding to requests for opinions, informing persons concerned and data controllers of their rights and obligations, authorizing certain sensitive processing, receipt of	**e –** Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State. **Articles 57 and 58** set out tasks and powers of supervisory authorities. Tasks	guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with	Supplementary Act. **Article 19: Responsibilities** – include informing data subjects and controllers of their rights and obligations, responding to requests for opinions, authorizing certain sensitive processing, dealing with claims, petitions and complaints, judicial referrals of offences, imposing administrative and financial sanctions, update a public register

	remedy before the supervisory authorities referred to, 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.		participate in the APEC Cross-border Privacy Enforcement Arrangement (CPEA) with a least one Privacy Enforcement Authority. Defines 'Privacy Enforcement Authority' as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforceme	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 mentioned in paragraph 1 of Article 1 of this Protocol.	proposals for any legislative or administrative measures which provide for the processing of personal data. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions		notifications of processing, dealing with claims, petitions, complaints, judicial referrals of offences, audits, imposing administrative and monetary sanctions, authorizing transborder transfers, establishing cooperation mechanisms. Authorities may also issue official warnings, followed by withdrawal of authorizations and	include monitoring and enforcement, handling complaints, promoting awareness, cooperating with other supervisory authorities. Powers include investigation, corrective powers, authorisation and advisory powers.	the appropriate individual remedies.	of personal data processing, authorizing transborder transfers, establishing cooperation mechanisms. Authorities may also issue warning notices, and formal demands to desist from violations, and require suspension of or prohibit processing. and monetary fines. **Article 20: Sanctions** – where a data processor does not conform, authorities can withdraw

			nt proceedings.	Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.	and exercise of their powers. Authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity.		monetary fines.			authorizations, and impose fines.
Compliance and monitoring: **Criteria on the independence of**	Supervisory authorities shall be impartial and independent, and will have technical competence, sufficient		**Cross-border Privacy Enforcement Arrangement** defines 'Privacy Enforcement	**Additional Protocol to the Convention for the Protection of Individuals with regard**	**Article 15: Supervisory authorities** – supervisory authorities shall act	**42. Nature of Control and Supervision Authorities** – Control authorities shall be free of any external	**Article 11: Status, composition and organization of National Personal Data Protection**	**Article 52: Independence** 1. Each supervisory authority shall act with complete	The authority shall offer guarantees of impartiality, and independence vis-à-vis persons or	**Article 16: Incompatibility** – membership of the data protection Authority shall be incompatible

supervisory authorities	powers and adequate resources to deal with claims by data subjects.		Authority' as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings	**to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows:** **Article 1 –** The supervisory authorities shall exercise their functions in complete independence.	with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.	influence and shall not request nor admit any order or instruction. Members 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 or each State, according to the rules of due process. Decisions of the control	**Authorities** – Each State Party shall determine the composition of the national personal data protection authority, but membership of the authority shall be incompatible with membership of Government, business executive and ownership of shares in the information and communication	independence. 2. The member or members of each supervisory authority shall remain free from direct and indirect external influence, and shall neither seek nor take instructions from anybody. 3. Member or members of each supervisory authority shall refrain from any action incompatible with their	agencies responsible for processing and establishing data.	with membership of government, the exercise of business executives, and ownership and shares in businesses in the information and telecommunications sectors. **Article 17: Immunity** – members shall enjoy full immunity in respect of opinions expressed in the exercise of, or during the tenure of their function. They shall receive no instructions

						authorities shall only be subject to jurisdictional control according to mechanisms in national legislation.	technologies sector. Members of the authority shall not receive instructions from any other authority in the performance of their duties.	duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not. 4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastruc-ture		from any Authority in discharging their duties.

								necessary for the effective perform-ance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participat-ion in the Board. 5. 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. 6. 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.		
Compliance and monitoring: **Cooperation with other authorities within the framework**	The competent supervisory authorities in each State will make every effort to share reports, investigation techniques, communication and regulatory strategies and any other useful information for exercising their functions more effectively, in particular when		Member economies are encouraged to share information re matters that have a significant impact on privacy protection, educate one another, share investigation techniques and regulatory strategies. **APEC Cross-border Privacy**	**Article 13: Cooperation between Parties** – the Parties agree to render each other mutual assistance in order to implement this Convention. **Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic**	**Article 17: Forms of cooperation** – The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties and exercise of their powers: including exchanging relevant and useful informatio	**45. Establishment of International Cooperation Mechanisms** – Ibero-American States may adopt international cooperation mechanisms, which may include: - mechanisms that allow reinforcing international assistance and cooperation in the application of		Article 57(g): Tasks – Supervisory authorities shall cooperate with, including sharing information and providing mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and		

	following a request for cooperation by another supervisory authority in conducting an investigation or intervention. Conduct coordinated investigations or interventions at national and international level where the interests of two or more authorities are shared. Take part in associations, working groups, joint fora, as well as seminars, workshops or		**Enforcement Arrangement (CPEA)** facilitates sharing and provides mechanisms to promote effective cross-border enforcement cooperation between authorities in APEC economies who have signed up to the arrangement. An economy must participate in the APEC Cross-border Privacy Enforcement Arrangeme	**Processing of Personal Data regarding supervisory authorities and transborder data flows:** **Article 1.5** In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent	n; cooperate with each other, coordinating investigations or interventions, conducting joint actions; providing information and documentation on law and administrative practice. Authorities shall form a network in order to organise their cooperation.	relevant national law. - assistance between control authorities through notification and submission of claims, assistance in investigations, and information exchange. - adoption of mechanisms aimed at awareness and exchange of best practices.		enforcement of the Regulation. Further detail is set out in **Articles 56: Competence of the lead supervisory authority**; **60: Cooperation between the lead supervisory authority and other supervisory authority**; **61: Mutual assistance** and **62: Joint operations of supervisory authorities**		

	courses that contribute to adopting joint positions or to improving the technical ability of the staff serving such supervisory authorities. Maintain appropriate level of confidentiality in respect of information exchanged in the course of cooperation.		nt (CPEA) with a least one Privacy Enforcement Authority.	necessary for the performance of their duties, in particular by exchanging all useful information.						
Compliance and monitoring: **Cooperation with other authorities outside the framework**	States should encourage the negotiation of cooperation agreements among international supervisory authorities that					**45. Establishment of International Cooperation Mechanisms** – Ibero-American States may adopt international	**Article 12: Duties and Powers of National Protection Authorities** – Authorities are responsible for establishing	**Article 50: International cooperation for the protection of personal data –** In relation to third countries		

/ between frameworks	contribute to more effective cooperation and coordination. Applicable national legislation may confer powers on the supervisory authorities to authorise some or all international transfers in their jurisdiction before they are carried out. Or be capable of demonstrating that the transfer complies with the guarantees provided for in the Madrid					cooperation mechanisms, which may include: - mechanisms that allow reinforcing international assistance and cooperation in the application of relevant national law. - assistance between control authorities through notification and submission of claims, assistance in investigations, and information exchange.	mechanisms for cooperation with the personal data protection authorities of third countries.	and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual		

	Resolution, and in particular where required by the supervisory authorities pursuant to the powers laid down under monitoring and compliance.					- adoption of mechanisms aimed at awareness and exchange of best practices.		assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;		

								(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and		

								practice, including on jurisdict-ional conflicts with third countries.		
Compliance and monitoring: **Cooperation monitoring body**					**Article 4.3 Duties of the Parties** Each Party undertakes: a. to allow the Convent-ion Committe e (…) to evaluate the effective-ness of the measures it has taken in its law to give effect			**Articles 63 – 76** set out the consistency mechanism in detail. The European Data Protection Board shall ensure the consistent application of the Regulation.		

					to the provisions of this Convent-ion; and b. to contribute actively to this evaluation process.					
Compliance and monitoring: **Liability**	The Responsible person will be liable for the pecuniary and non-pecuniary damages caused to the data subjects, except if the responsible person can demonstrate the damage is not attributable to him. This liability is without				**Explanatory Report: Article 99** – In order for the Convention to guarantee an effective level of data protection, the duties of the controller and processor and the	Implied in **Article 44: Restitution** – sets out a right to compensation in the event of violation of data protection rights.		**Article 82: Right to compensation and liability** - Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be		

	prejudice to any action by the responsible person against the processing service provider involved at any stage of the processing.				rights of data subjects should be reflected in the Parties' legislation with correspon ding sanctions and remedies. **Article 100** It is left to each Party to determine the nature (civil, administra tive, criminal) of these judicial as well as non-judicial sanctions.			liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. A controller or processor shall be exempt from liability if it proves that it is not in		

					These sanctions have to be effective, proportio nate and dissuasive. The same goes for remedies: data subjects must have the possibility to judicially challenge a decision or practice, the definition of the modalities to do so being left with the Parties. Non-judicial remedies			any way responsible for the event giving rise to the damage.		

					also have to be made available to data subjects. Financial compensation for material and non-material damages where applicable, caused by the processing and collective actions could also be considered.					
Compliance and monitoring:			Member economies should include appropriate remedies	**Additional Protocol to the Convention for the Protection**	**Article 15: Supervisory authorities** – Each compet-	**43. Claim and Sanction Regime** – holders have the right to submit claims		**Article 77: Right to lodge a complaint with a supervisory**	May be possible: In the event of violation of the provisions of	

Data subject redress before supervisory authorities			for privacy violations – could include redress, depending on the system in that member economy.	**of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows:** **Article 1 –** Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the	ent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of their progress. **Article 18 – Assistance to data subjects** Each Party shall assist any data subject,	before the control authority to make their rights effective in accordance with national legislation.		**authority –** Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers	the national law implementing the principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.	

				processing of personal data within its compet-ence.	whatever his or her nationality or residence, to exercise his or her rights under Article 9 of this Conventio n.			that the processing of personal data relating to him or her infringes this Regulation.		
Compliance and monitoring : **Data subject redress in court against the controller:** **- administrat ive** **- judicial**	Without prejudice to any administrative remedy before the supervisory authorities, referred to above, including judicial oversight of their decisions, data subjects may have a direct		Dependent on system in the member economy, remedies could include rights of individuals to pursue legal action.	May be possible: **Article 10: Sanctions and remedies –** Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving	May be possible: **Article 12: Sanctions and remedies –** Each Party under-takes to establish appro-priate judicial and non-judicial sanctions and	May be possible: **43. Claim and Sanction Regime** – holders have the right to due process of law to make their rights effective in accordance with national legislation.		**Article 79: Right to an effective judicial remedy against a controller or processor –** Without prejudice to any available administrati ve or non-judicial remedy, including	May be possible: In the event of violation of the provisions of the national law implement-ing the principles, criminal or other penalties should be envisaged together with the	

	recourse to the courts to enforce their rights under the provisions laid down in the applicable national legislation.			effect to the basic principles for data protection.	remedies for violations of the provisions of this Conventio n. Under **Article 9**, data subjects have a right to have an Article 12 remedy and to benefit, whatever his or her nationality or residence, from the assistance of a super-visory authority within the meaning of Article 15, in			the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance	appropriate individual remedies.	

					exercising his or her rights under this Convent-ion.			with this Regulation. **Article 82: Right to compensati on and liability –** Any person who has suffered material or non-material damage as a result of an infringe-ment of this Regulation shall have the right to receive compens-ation from the controller or processor for the damage suffered.		

Compliance and monitoring: **Collective actions**					**Explanatory Report: Article 100 –** It is left to each Party to determine the nature (civil, administrative, criminal) of these judicial as well as non-judicial sanctions. These sanctions have to be effective, proport-ionate and dissuasive. The same goes for remedies: data subjects must have			**Article 80: Representation of data subjects –** The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the		

					the possibility to judicially challenge a decision or practice, the definition of the modalities to do so being left with the Parties. Non-judicial remedies also have to be made available to data subjects. Financial compensation for material and non-material damages			protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where		

					where applicable, caused by the processing and collective actions could also be consid-ered.			provided for by Member State law. Member States may also provide that any such body, organis-ation or association, independ-ently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority.		
Compliance and				**Additional Protocol to the Convention**	**Article 15: Supervisor y authoritie**	**Article 42.5: Nature of Control and Supervision**	**Article 12: Duties and Powers of National**	**Article 78: Right to an effective judicial**		

monitoring: **Actions against the supervisory authorities**				**for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows:** **Article 1.4 –** Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.	**s** – Decisions of the supervisory author-ities may be subject to appeal through the courts.	**Authorities** – gives scope for this according to applicable national legislation.	**Protection Authorities** – The sanctions imposed and decisions taken by national protection authorities are subject to appeal.	**remedy against a supervisory authority –** 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. Each data subject shall have the right to an effective judicial remedy where the supervisory authority		

								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.		
Compliance and monitoring: **Administrative fines**				May be possible: **Article 10: Sanctions and remedies –** Each Party undertakes to establish appropriate sanctions and remedies for violations of	**Article 15: Supervisory authorities** – supervisory authorities shall have powers to issue decisions with respect to	**43. Claim and Sanction Regime** – national legislation shall establish a regime that allows the adoption of corrective measures, and to sanction conducts that	**Article 12: Duties and Powers of National Protection Authorities –** National protection authorities are responsible for imposing administrative and monetary	Administrative fines are available for supervisory authorities to issue. **Article 83** sets out general conditions for imposing such fines.	May be possible: In the event of violation of the provisions of the national law implementing the principles, criminal or other penalties should be	**Article 19: Responsibilities** – Authorities can impose administrative and financial sanctions on data controllers. **Article 20: Sanctions** Where a data processor does not

				provisions of domestic law giving effect to the basic principles for data protection.	violations of the provisions of this Conventio n and may, in particular, impose administra tive sanctions.	contravene national law. It should state the maximum limit and the objective criteria for establishing the relevant sanctions.	sanctions on data controllers.		envisaged together with the appropriate individual remedies.	conform, authorities may issue a fine.
Compliance and monitoring : **Penalties**				May be possible: **Article 10: Sanctions and remedies –** Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to	**Article 15: Supervis- ory authorit- ies** – super- visory author- ities shall have powers to issue decisions with respect to violations of the provisions of this	**43. Claim and Sanction Regime** – national legislation shall establish a regime that allows the adoption of corrective measures, and to sanction conducts that contravene national law. It should state the	**Article 12: Duties and Powers of National Protection Authorities –** National protection authorities are responsible for imposing administrativ e and monetary sanctions on data controllers. Authorities	**Article 84: Penalties –** Member States shall lay down the rules on other penalties applicable to infringemen ts of this Regulation in particular for infringemen ts which are not subject to administ-	May be possible: In the event of violation of the provisions of the national law implementin g the principles, criminal or other penalties should be envisaged together with the appropriate	

				the basic principles for data protection.	Convent-ion and may, in particular, impose administ-rative sanctions.	maximum limit and the objective criteria for establishing the relevant sanctions.	may issue warnings, temporary or permanent withdrawals of authorizations, and make decisions to discontinue, block or prohibit processing.	rative fines, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportion-ate and dissuasive.	individual remedies.	
Cross-border transfers										
General principles relating to international transfers:	As a general rule, international transfers of personal data may be carried out when the State to which	16. A data controller remains accountable for personal data under its control	Member economies should refrain from restricting cross-border flows between	**Article 12: Transborder flows of personal data and domestic law**	**Article 14: Transborder flows of personal data** - **Between member countries**	**36. General Rules for Transferring Personal Data** – International transfers can take place if:		**Article 44: General principle for transfers –** Any transfer of personal data which	**Transborder data flows** – When the legislation of two or more countries concerned by a transborder data flow	**Article 36: Transfer of personal data to a non-member ECOWAS country** – the data controller

- between member countries **- outside the framework**	such data are transmitted affords as a minimum, the level of protection provided for in the Madrid Resolution.	without regard to the location of the data. 17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards	themselves and other member economies where the other economy has in place legislative or regulatory instruments that give effect to the Framework, or where sufficient safeguards exist. **The Cross-Border Privacy Rules System** is a practical mechanism for APEC economies to transfer personal information across-borders.	A Party shall not, for the sole purpose of privacy protection, prohibit/ subject to special authorisation transborder data flows to another Party. Parties can derogate from this provision where its legislation includes specific regulations for certain data categories, unless the other Party's regulations provide	A Party shall not, for the sole purpose of privacy protection, prohibit/ subject to special authorisation transborder data flows to another Party – unless there is a real and serious risk that the transfer (or any onward transfers to non-Parties) would lead to circumven	- the country/territory/sector/ activity/ international organisation/ recipient has an appropriate level of protection of personal data (acknowledged by the transferring country) - Exporter offers sufficient guarantees for the treatment of personal data in the recipient country and the recipient proves compliance. - contractual clauses/other		are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor,	offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.	shall transfer personal data to a non-member ECOWAS country only where an adequate level of protection for privacy, freedoms and the fundamental rights of individuals exists. The data controller shall inform the data protection authority prior to any transfer of personal data to such a third country.

		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. 18. Any restrictions to transborder flows of personal data should be	Member economies should encourage and support the development of international arrangements that promote interoperability amongst privacy instruments that give practical effect to the Framework.	equivalent protections; or when a Party will transfer through the intermed-iary of another Party to a non-Contracting State. **Outside the framework:** see additional Protocol CETS 181 – Article 2.	ting the provisions of the Convention or if a Party is bound by harmonised rules of protection shared by States belonging to a regional international organisation... **Explanatory Report: Article 106** There might, however, be exceptional cases where there is a	legal instrument that offers sufficient guarantees. - Exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism. - Transfer authorised by the control authority of the Ibero-American State of the exporter.		including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.		

		proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.			real and serious risk that this free circulation of personal data will lead to the circumvention of the provisions of the Convention. As an exception, this provision has to be interpreted restrictively and Parties cannot rely on it in cases where the risk is either hypothetic					

					al or minor. - **outside the framework** the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convent-ion is secured (listed in Article 14, including State laws; ad hoc or approved standard-ised					

					safeguards provided by legally binding and enforce-able instru-ments; in specific cases: data subject consent, require-ment of the interests of the data subject, prevailing legitimate interests if provided for by law and such transfer constitute s a necessary and					

					proportionate measure in a democratic society, or constitutes necessary and proportionate measures in a democratic society for freedom of expression.)					
Mechanisms: **Adequacy of recipient states**	The notion of adequacy is implied, but no specific mechanism is set out.	The notion of adequacy is implied, but no specific mechanism is set out.			Appropriate levels of protection for transfers can be based on State laws or ad hoc	**36. General Rules for Transferring Personal Data** – International transfers can take place if:		**Article 45: Transfers on the basis of an adequacy decision –** A transfer of personal data to a third	The notion of adequacy is implied, but no specific mechanism is set out.	The notion of adequacy is implied, but no specific mechanism is set out.

					or approved standardised safeguards provided by legally-binding and enforceable instruments. **Article 23.f** The Convent-ion Comm-ittee may, at the request of a State or an intern-ational organis-ation, evaluate whether the level of personal	- the country/territory/sector/ activity/ international organisation/ recipient has an appropriate level of protection of personal data (acknowledged by the transferring country). No specific mechanism is set out.		country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the inter-national organis-ation in question ensures an adequate level of protection. Such a transfer		

					data protection the former provides is in compliance with the provisions of this Convention and, where necessary, recommend measures to be taken to reach such compliance.			shall not require any specific authorisation. Elements for the Commission to take account of when assessing adequacy are specified.		
Mechanisms : **Approved self-assessment schemes for organisations**			**The Cross-Border Privacy Rules System** – a practical mechanism for APEC economies to transfer personal		**Article 23 g** The Convention Committee may develop or approve models of	**36. General Rules for Transferring Personal Data –** International transfers can take place if the exporter and recipient				

			information across-borders.		standardised safeguards referred to in Article 14.	adopt a binding self-regulation scheme or an approved certification mechanism. No such schemes are specified.				
Mechanisms: **Binding Corporate Rules (BCRs)**	If States do not afford the level of protection provided for in the Madrid Resolution, transfers can be made where those who expect to transmit such data guarantee that the recipient will afford such level of protection. In particular, where the				No specific mention of BCRs, but **Article 14.3.b.** suggests that ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted	**36. General Rules for Transferring Personal Data** – International transfers can take place if (…) - Exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism. No specific mention of BCRs.		**Article 46(2)(b): Transfers subject to appropriate safeguards –** Personal data to a third country or international organisation only be transferred if appropriate safeguards are in place. One specified		

	transfer is carried out within corporations or multinational groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory.				and implemented by the persons involved in the transfer and further processing can provide an appropriate level of protection.			safeguard is binding corporate rules in accordance with Article 47. **Article 47: Binding corporate rules –** the competent supervisory authority shall approve binding corporate rules as set out in Article 47, to enable transfers within multinational companies.		
Mechanisms:						**36. General Rules for Transferring Personal**		**Article 46(2)(e): Transfers subject to**		

Codes of Conduct						**Data** – International transfers can take place if (...) - Exporter offers sufficient guarantees for the treatment of personal data in the recipient country and the recipient proves compliance. (…) - Exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism.		**appropriate safeguards –** Personal data to a third country or international organisation only be transferred if appropriate safeguards are in place. One specified safeguard is an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or		

								processor in the third country to apply the appropriate safeguards. **Article 40: Codes of Conduct** – sets out that approved codes of conduct can be used to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to		

								in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.		
Mechanisms: **Contractual Clauses**	If States do not afford the level of protection provided for in the Madrid				**Article 14** Appropriate levels of protection for transfers	**36. General Rules for Transferring Personal Data –** International		**Article 46(2)(c),(d) and (3): Transfers subject to appropriate**		

	Resolution, transfers can be made where those who expect to transmit such data guarantee that the recipient will afford such level of protection. Guarantees could result from appropriate contractual clauses.				can be based on approved standardised safeguards provided by legally binding and enforce-able instru-ments. This could result in the use of mechan-isms such as contract-ual clauses, but no specific mechan-ism is set out.	transfers can take place if the exporter and recipient sign contractual clauses/other legal instrument that offers sufficient guarantees.		**safeguards –** Personal data to a third country or inter-national organis-ation only be transferred if appropriate safeguards are in place. One specified safeguard is standard data protection and contractual clauses		
Mechanisms:						**36. General Rules for Transferring**		**Article 46(2)(f): Transfers**		

Certification						**Personal Data –** International transfers can take place if the exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism. No specific mechanisms are set out.		**subject to appropriate safeguards –** Personal data to a third country or international organisation only be transferred if appropriate safeguards are in place. One specified safeguard is approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or		

								processor in the third country to apply the appropriate safeguards. Article 42 sets out require-ments for certification mechanism.		
Mechanisms: **Administrative arrangements**					No specific mention of administrative arrangements, but **Article 14.3.b.** suggests that ad hoc or approved standardised safeguards provided by legally-	**36. General Rules for Transferring Personal Data** – International transfers can take place if (…) - Exporter offers sufficient guarantees for the treatment of personal data in the recipient		**Article 46(3): Transfers subject to appropriate safeguards** - Subject to the authorisation from the competent supervisory authority, the appropriate safeguards may be provided for, in		

					binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.	country and the recipient proves compliance. - signed contractual clauses/other legal instrument that offers sufficient guarantees. - Exporter and recipient adopt a binding self-regulation scheme or an approved certification mechanism. No specific arrangements set out.		particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organis-ation; or (b) provisions to be inserted into administ-rative arrangemen		

								ts between public authorities or bodies which include enforceable and effective data subject rights.		
Derogations	National legislation applicable to those who expect to transmit data may permit an international transfer of personal data to States that do not afford the level of protection provided for in the Madrid Resolution, where necessary in			Parties can derogate from the provision of not prohibiting or subjecting to special authorisation transfers to another Party where its legislation includes specific regulations for certain data	**Article 14.1** 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a	**36. General Rules for Transferring Personal Data** – Ibero-American State national law may expressly establish limits to international transfers of categories of personal data, for reasons of national security,		**Article 49: Derogations for specific situations –** if no adequacy decision or appropriate safeguards apply, a number of derogations are available, such as explicit consent, performance of a		

	the interest of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public interest grounds.			categories, unless the other Party's regulations provide equivalent protections; or when a Party will transfer through the intermediary of another Party to a non-Contracting State.	recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so 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	public security, public health protection, protection of rights and freedoms of third parties, and public interest matters.		contract, public interest, establishment, exercise or defence of legal claims, vital interests.		

					Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation. **Explanatory Report: Article 106** There might, however, be exceptional cases where there is a real and serious					

					risk that this free circulation of personal data will lead to the circumvention of the provisions of the Convention. As an exception, this provision has to be interpreted restrict-ively and Parties cannot rely on it in cases where the risk is either hypoth-etical or minor.					

Onward transfers to third countries				Parties can derogate from the provision that a Party shall not, for the sole purpose of privacy protection, prohibit/ subject to special authorisation transborder data flows to another Party, when a Party will transfer through the intermediary of another Party to a non-Contracting State.	Parties can prohibit or subject to special authorisation transborder data transfers if there is a real and serious risk that the transfer from the other Party to a non-Party would lead to circumventing the provisions of the Convent-ion. **Explanatory Report:**			**Article 44: General principle for transfers –** Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the		

					Article 106 There might, however, be exceptional cases where there is a real and serious risk that this free circulation of personal data will lead to the circumvention of the provisions of the Convention. As an exception, this provision has to be interpreted			conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter		

					restrictively and Parties cannot rely on it in cases where the risk is either hypothetical or minor.			shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.		

Annex 2: GPA referential on convergence between global data protection frameworks

GPA referential on convergence between global data protection frameworks

Introduction

The 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC, now the GPA) adopted a Resolution on the Conference's Strategic Direction, which set out as a strategic priority the need to work towards a global regulatory environment with clear and consistently high standards of data protection. In the same Resolution, the GPA adopted a Policy Strategy that mandated the Assembly to carry out work focused on the theme of evolution towards global policy, standards and models.

As part of that work, an analysis of ten global privacy and data protection frameworks was carried out, which identified a strong degree of commonality and convergence between them. All frameworks cover both public and private sectors and this document highlights the identified commonalities and convergence between the frameworks. In particular it sets out those common fundamental principles and core elements, which not only suggest a commitment to shared values, but also provide a point of reference for GPA members in their conversations with those they regulate, their governments and wider global stakeholders.

The analysis indicated strongly that although different legal, constitutional and cultural approaches to data protection and privacy exist, there are global values that can work within all. It reflected an almost universal acceptance of a number of key principles and rights; and further elements that, while not attracting universal agreement, reflected relatively broad acceptance of increasingly important privacy protections in today's global environment. This document brings these core principles, rights and themes together.

Core principles

- Fairness

  The processing of personal data should not result in unlawful or arbitrary discrimination. Any processing of personal data should be within individuals' reasonable expectations and should be justifiable. Individuals should not be misled about any aspect of the processing of their personal data.

- Lawfulness

  The processing of personal data must not be unlawful and should respect any applicable national legislation. Where appropriate to the jurisdiction, processing of personal data should have a specific basis in law.

In particular, where consent is an appropriate basis for legitimising processing, it should be freely given, specific, fully informed and unambiguous.

- Purpose specification

  Those organisations or individuals processing personal data should specify the purposes for the processing. The processing of personal data should be limited to fulfilling the specified, explicit and legitimate purposes.

- Proportionality

  The processing of personal data should be limited to that which is adequate, relevant and necessary in relation to the specified purpose. Processing should be limited to the minimum necessary to fulfil that purpose.

- Data quality

  Personal data processed should be accurate, complete and up to date to the extent required for the purpose.

- Openness and transparency

  Transparency is vitally important in enabling individuals to make informed decisions about whether and how they interact with organisations, and exercise their rights. Those responsible for processing personal data should have transparent policies in place with regard to the processing. They should be honest and open, and in particular actively provide information to those individuals whose data is processed, in simple and clear language. This information should include, as a minimum, the identity of the organisation processing the personal data, the purposes for processing, the source of the data, recipients, data subject rights and how they can be exercised.

- Security

  Appropriate technical and organisational measures must be taken to protect personal data, to preserve its integrity, confidentiality and availability. The measures taken should be appropriate to the risk inherent in the processing, taking into account, for example, the nature of the data, the possible consequences of a security incident, and the state of technology.

- Data retention

  Data should be retained for the minimum necessary period in relation to the purpose. When data is no longer necessary for the legitimate stated purpose it should be deleted or rendered anonymous.

- Accountability and responsibility

  Those responsible for processing personal data should be accountable and liable for complying with the applicable principles to the processing. They must have the necessary processes, procedures and mechanisms in place in order for them to be able to sustainably demonstrate compliance with the principles and obligations set out in the applicable privacy and data protection legislation. Such mechanisms might include, for example, Data Protection Impact Assessment, privacy management programmes, audits, breach prevention and notification, and training.

- Privacy by design

  It is vital to ensure that privacy is actively and carefully considered from the outset when developing new technologies, implementing new systems, services, products and business practices. This should include identifying the required data, how it will be used and any risks that the processing raises, putting effective measures in place to mitigate them. This may require consultation and engagement with the public and with regulators.

- Cross-border transfers – general protection requirements

  The ability to transfer personal data across-borders is vital for many functions of the global economy. Effective safeguards must be in place when transferring personal data across-borders, in accordance with applicable laws in each jurisdiction. Organisations should remain accountable for personal data under their control regardless of the location.

Error! Bookmark not defined.

- Access

  The right of access to personal data is a fundamental cornerstone of privacy and data protection, allowing individuals to understand how and why their data is being used, and to check it is being used legitimately. Individuals should therefore be able to obtain information as to whether their personal data is being processed, and if so, to have that data communicated to them on request.

- Objection/opposition

  Wherever possible, individuals should be able to exercise choice over the processing of their personal data. They should therefore have the right to object to the processing of their personal data.

- Rectification

  There is a risk to individuals if the personal data processed about them is inaccurate, incomplete or out of date. Individuals should therefore have the right to have personal data rectified where this is the case.

- Deletion/erasure

  Individuals should have the right to request the deletion or erasure of personal data.

Special requirements

- Specific requirements for sensitive data

  Certain types of data should be classified as sensitive, or special. This should include data that would affect the data subject's most intimate sphere, or data that, if misused, would be likely to give rise to discrimination or other serious risks to the data subject, as appropriate in each jurisdiction. Examples could be data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life.

- Specific requirements for the processing of children's or vulnerable individuals' data

  Whilst most frameworks did not set out specific requirements for children or vulnerable adults, the volume of work on the topic of children's privacy being undertaken by authorities and other organisations reflects a developing recognition that children and vulnerable adults may need particular protection when their personal data is processed. This is because they may be less aware of, or have a lesser understanding of, the risks involved. This particular protection need should be considered at the outset of any plans to process their personal data, and systems and processes should be designed and operated accordingly, with additional protections as necessary.

- Specific requirements for automated decisions taken using personal data

  Whilst most frameworks did not set out specific requirements for automated decisions, the application of the more universally agreed principles to automated decisions taken using newer technologies can require such context-specific considerations. As newer technologies such as artificial intelligence are more widely employed, there is potential for increased numbers of automated decisions being taken, using increasing volumes of personal data, for a broader range of purposes. This could include the profiling of individuals, which can carry a high privacy risk. Any solely automated decision taken, or profiling carried out, using personal data should therefore be subject to strong safeguards, including privacy and data protection by design, alongside transparency and explainability, that are effective in the digital environment.

The role of data protection and privacy enforcement authorities

- Establishment of independent supervisory or enforcement authority

It is vital that a supervisory or enforcement authority is in place, and that it is independent and impartial. Authorities should have the necessary resources available, and sufficient powers to supervise and enforce the applicable laws and frameworks. Individuals should be able to obtain redress before a supervisory or enforcement authority and/or a court in case their privacy rights are infringed.

- Cooperation between data protection and privacy enforcement authorities

  Regulatory cooperation between authorities should take place when cross-border actions are needed to protect personal data. This is of vital importance as the processing of personal data has an increasingly global nature, as technology develops and multinational organisations process the personal data of citizens across-borders. Mechanisms for mutual assistance and international enforcement cooperation with other authorities, which support the ability to both send and receive data while ensuring compatibility with relevant investigative or legally privileged requirements, should be developed, with an aim of ensuring privacy rights can be exercised, complaints can be pursued and investigations carried out by an appropriate authority wherever the organisation responsible for the processing is based.