

# Policy Strategy Working Group 1: Global frameworks and standards

Report – adopted October 2020

Chair authority: UK ICO

Table of Contents	Page
Executive Summary	3
Introduction	5
Working group activities	6
Forward looking plan 2020-21	12
Conclusion	13
Annexes	14

## **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<sup>1</sup> at the 41<sup>st</sup> 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 Internationa Authority (observe		European Commis	sion (observer)	EDPB (observer)

<sup>&</sup>lt;sup>1</sup> 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."<sup>2</sup>

### 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.

<sup>&</sup>lt;sup>2</sup> 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 31 <sup>st</sup> 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 internationall y uniform protection of privacy with regard to the processing of personal data:		- Promoting e- commerce throughout the Asia- Pacific regionEncourage 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 accomplish ment 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 informatio n in the Asia Pacific region.	fundamenta I freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to his "data protection".	data, thereby contributi ng to respect for his or her human rights and fundamen tal 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	and social progress, to the strengthening and the convergence of the economies within the internal market, and to the wellbeing of natural persons.		personal data without prejudice to the general interest of the State.
--	--	--	---	---	--	---	--	---

							framework aimed at strengthenin g 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 suppleme nted by additional measures for the protection of privacy and individual	A set of principles and guidelines — to be implement ed as each member economy determines . The framework states there should be flexibility in implementing the principles,	Internation al convention — binding when ratified.	Internatio nal conventio n – binding when ratified. Provisiona I applicatio n is possible upon declaratio n (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	Supplementar y Act to the ECOWAS Treaty — binding on Member States.

		liberties, which may impact transbord er flows of personal data.	in view of different social, cultural, economic and legal background s of member economies.		Lithuania and Norway³). Partial entry into force possible from 2023 with 38 ratificatio ns (full entry into force when all Parties to Conventio n 108 will have ratified).				and regulations.	
Material	Any	Guidelines	Applies to	Applies to	Applies to	Applies to	Applies to	Article 2	Field of	Article 3:
scope	processing of personal data,	apply to personal	the collection,	the automated	the	the treatment of	any collection,	The Regulation	application Principles	Scope Collection,
	wholly or	data,	holding,	processing	processing of	personal data	processing,	applies to	should be	processing,
	partly by	whether	processing,	of personal	personal	of individuals	transmission,	the	applicable to	transmission,
	automatic	in the	use, transfer or	data in both	data in	contained in	storage or	processing	all public and	storage, and
	means, or	public or	disclosure	public and	both	physical, fully	use of	of personal	private	use of
	otherwise in a	private	of personal	private	public and	or partially or	personal data	data, either	computerize	personal data
	structured manner and	sectors, which,	informatio	sectors. Parties can	private	both,	by a natural	wholly or	d files as well	by any
	manner and	willell,	n about	raities tall	sectors,	automated	person, the	partly by	as, by means	individual, by

 $<sup>^3\,</sup> See: \underline{https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/declarations?p\ auth=h61bPRI5}$ 

carried out in	because of	natural	declare the	subject to	media,	State, local	automated	of optional	government
		living			•	1		•	government,
both the	the	persons.	Convention	each	regardless of	communities,	means, and	extension	local
public and	manner in		does not	Party's	the form or	and public or	to non-	and subject	authorities,
private	which	Limited	apply	jurisdictio	modality of	private	automated	to	and public or
sectors,	they are	application	(exclusion)	n.	their	corporate	processing	appropriate	private legal
subject to	processed,	to publicly	or it does	It does not	creation,	bodies.	of personal	adjustments,	entities shall
each Party's	or	available	apply	apply to	type of	Any	data which	to manual	be subject to
jurisdiction.	because of	informatio	(extension)	data	media,	automated	form part of	files. States	this
	their	n.	to certain	processing	processing,	or non-	or are	can opt to	Supplementar
	nature or		categories	carried	storage and	automated	intended to	extend all or	y Act.
	the		of files.	out by an	organization.	processing of	be part of a	part of the	
	context in			individual		data	filing	principles to	
	which			in the		contained in	system.	files on legal	
	they are			course of		or meant to	Does not	persons	
	used, pose			purely		be part of a	apply to the	particularly	
	a risk to			personal		file.	processing	when they	
	privacy			or		THE.	of personal	contain some	
	and			household			data for	information	
	individual			activities.			activities	on	
	liberties.			detivities.			falling	individuals.	
							outside the		
							scope of EU		
	In federal						law such as:		
	countries						iaw sucii as.		
	the						(a) in the		
	observanc						course of an		
	e of these						activity		
	Guidelines						which falls		
	may be						outside the		
	affected						scope of		
	by the						Union law;		
	division of								

		powers in the federation						(b) for purely personal and household activities; (c) by competent authorities for criminal investigatio n, detection, prosecution .		
Scope	Both private	Both	Framework	Both	Both	Both public	Both public	Both	Both private	Both private
includes	and public	private	<ul><li>both</li><li>private and</li></ul>	private and	private	and private	and private	private and	and public	and public
private sector and	sectors.	and public sectors.	public	public sectors.	and public sectors.	sectors. Standards	sectors.	public sectors.	sectors.	sectors.
public		350013.	sectors,	3661013.	3501013.	apply to	Applies to	3661013.		
authorities,	Restrictions in		however it			individuals,	any		Principle 6:	Processing []
including	the interests	Exceptions	should be noted that:	Derogation	Exceptions	private legal	collection,	Does not	Power to	by any
governmen	of national	to the		from	allowed to	entities,	processing, transmission,	apply to	make	individual, by
t?	security,	Guidelines	- it is not intended to	certain	certain	authorities	storage or	issues	exceptions.	government,
	public safety,	should be as few as	impede	articles allowed	Articles when such	and public bodies.	use of	which fall outside the	Departures from	local
National	protection of public health	possible	governmen	when	an	boules.	personal data	scope of EU	principles 1	authorities, and public or
security?	or rights and	but may	t activities	provided	exception		by a natural	law, e.g.	to 4 may be	private legal
,	freedoms of	relate to	authorized by law	for by the	is	National	person, the	national	authorized	entities shall
	other should	national	when taken	law of the	provided	legislation	State, local communities,	security.	only if they	be subject to
	be expressly	sovereign-	to protect	Party and	for by law,	may limit the	communices,		are necessary	this

provided by	+1/	national	constitutes	rocposts	right to the	and public or	to protect	Supplementar
1 .	-ty,	security.		respects	_	· ·	to protect	I
national	national 	security.	a necessary	the	protection of	private	national 	y Act.
legislation.	security	- the <b>Cross-</b>	measure in	essence of	data in order	corporate	security,	Applies to any
	and public	Border	а	the	to safeguard	bodies.	public order,	processing of
	policy	Privacy	democratic	fundamen	national		public health	data related
	("ordre	Rules	society in	tal rights	security,		or morality,	to public
	public").	System	the	and	public	Any	as well as,	security,
		applies	interests of	freedoms	security,	processing of	inter alia, the	defence,
		only to the	protecting	and	public health	data relating	rights and	•
		personal	State	constit-	protection,	to public	freedoms of	investigation and
		data	security,	utes a	the	security,	others	
		processing	public	necessary	protection of	defence,	[]provided	prosecution of
		of business organizatio	safety, the	and	rights and	research,	that such	criminal
		ns, not	monetary	proport-	freedoms of	criminal	departures	offences or
		governmen	interests of	ionate	third parties,	prosecution	are expressly	State security,
		ts or	the State or	measure	as well as	or State	specified in a	subject to
		individuals.	the	in a demo-	due public	security may	law or	such
			suppression	cratic	interest	be subject to	equivalent	exemptions as
			of criminal	society	matters.	exceptions	regulation	are defined by
			offences,	for:	Limitations	defined by	promulgated	specific
			protecting		and	specific	in	provisions
			the data	a. the	restrictions	provisions of	accordance	stipulated in
			subject or	protection	shall be	other extant	with the	other legal
			the rights	of national	expressly	laws.	internal legal	texts in force.
			and	security,	acknowledge	laws.	system which	
				defence,	_		•	
			freedoms of	public	d in the law.		expressly	
			others.	safety,			states their	
				important			limits and	
				economic			sets forth	
				and			appropriate	
				financial			safeguards.	

	interests	
	of the	
	State, the	
	impartialit	
	y and	
	independe	
	nce of the	
	judiciary	
	or the	
	preventio	
	n,	
	investigati	
	on and	
	prosecutio	
	n 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 fundamen tal freedoms of others, notably freedom of expression				
Territorial scope	Member countries are recomme nded to implemen t 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 internatio nal organisati on may, at the time of signature / ratificatio n 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 Conventio n shall apply. (Such declaratio n 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	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
		established in the territory but to whom the	in the Union, where the processing
		such States applies by a person responsible or in charge, not	to: - the offering of goods or services to such data
		established in the territory but	subjects in the Union.

|--|

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 informatio n' – any informatio n about an identified or identifiable individual.	'Personal data' – any information relating to an identified or identifiable individual.	'Personal data' – any informatio n relating to an identified or identifiabl e individual.	'Personal data' – any information regarding an individual identified or identifiable.	'Personal data' – any information relating to an identified or identifiable natural person.	rpersonal 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	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

corruing out	0.0	20000	moone such	not by	obtaining
carrying out	on,	access,	means, such	not by	obtaining,
of logical	alteration,	registration,	as the	automated	using,
and/or	retrieval,	organisation,	collection,	means,	recording,
arithmetical	disclosure,	structuring,	recording,	such as	organisation,
operations	making	adaptation,	organization,	collection,	preservation,
on those	available,	indexation,	storage,	recording,	adaptation,
data, their	erasure,	modification,	adaptation,	organisatio	alteration,
alteration,	or	extraction,	alteration,	n,	retrieval,
erasure,	destructio	consultation,	retrieval,	structuring,	saving,
retrieval or	n of, or	storage,	backup, copy,	storage,	copying,
disseminati	the	preservation,	consultation,	adaptation	consultation,
on.	carrying	development	use,	or	utilisation,
	out of	, transfer,	disclosure by	alteration,	disclosure by
	logical	disseminatio	transmission,	retrieval,	transmission,
	and/or	n,	disseminatio	consultatio	dissemination
	arithmetic	possession,	n or	n, use,	or otherwise
	al	exploitation,	otherwise	disclosure	making
	operations	and, in	making	by	available,
	on such	general any	available,	transmissio	alignment or
	data.	use or	alignment or	n,	combination,
		disposal).	combination	disseminati	as well as
			and locking,	on or	blocking,
			encryption,	otherwise	encryption,
			erasure or	making	erasure or
			destruction.	available,	destruction of
				alignment	personal data.
				or	
				combinatio	
				n,	
				restriction,	

<sup>&</sup>lt;sup>4</sup> https://rm.coe.int/16807096c3

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

		concernin g her or him or for analysing or predicting her or his personal preferenc es, behaviour s and attitudes. (NB not legally binding).			
Pseudonym isation		18 of the Explanato ry Report refers to 'pseudony mous' data.	Not strictly defined, but Article 2.1.a defines anonymizatio n broadly, as 'the application of measures of any kind aimed at preventing the identification or re-	'Pseudony misation' – 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 disproportion ate efforts.'		without the use of additional information , provided that such additional information is kept separately and is subject to technical and organisatio nal measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	
Controller	(Doononsible	/Data	(Dorsonal	(Controller	(Cantrallar	(Dayson	(Data	person.	(Data
Controller	'Responsible person' – means any natural	'Data controller' – a party who,	'Personal informatio n 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	'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 competen t to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminat ed by that party or by an agent on its behalf.	organisatio n who controls, or instructs another, to collect, hold, use, process, transfer or disclose personal informatio n.	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.  or the processor are authorized to 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 communicati on of such data other than the data subject, the data controller, the subcontractor and persons who, for reasons of their functions,  'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Does not include public authorities	'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 responsibilit to process the data.	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	Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambigu ous 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 manifestatic n of express unequivocal free, specific and informe will by which the data subject or his/her legal judicial or treaty representation e accepts that his/her personal data be subjected.	of the data subject – any freely given, specific, informed and unambiguo us indication of the data subject's wishes by which he or she, by a	'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	of some	to manual or	affirmative	manually or
data subjects	other	electronic	action,	electronically.
to withdraw	legitimate	processing.	signifies	,
their consent	basis laid		agreement	
at any time	down by		to the	
and that shall	law.		processing	
not entail			of personal	
undue delay			data	
or cost, nor	Explanato		relating to	
gain for the	ry report		him or her.	
responsible	paragraph			
person.	<b>42</b> The			
l' l	data			
	subject's			
	consent			
	must be			
	freely			
	given,			
	specific,			
	informed			
	and			
	unambigu			
	ous. Such			
	consent			
	must			
	represent			
	the free			
	expression			
	of an			
	intentiona			
	I choice,			
	given			

Demonal	either by a statement (which can be written, including by electronic means, or oral) or by a clear affirmativ e action and which clearly indicates in this specific context the acceptanc e of the proposed processing of personal data.	Article 4	
Personal Data Breach	Defined in Article 22.1 as 'a violation to the safety		

					of personal dataunderstood 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, unauthorise d disclosure of, or access to, personal data transmitted , stored or otherwise processed.	
Supervisory Authority	'Privacy enforcem ent authority' - any public body, as determine d by each Member country, that is	Enforceme nt Authority' — any fublic body responsible for enforcing privacy laws and that has	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 authoritie s to be responsible for ensuring complianc	Not fully defined but clearly referred to in Article 42: 'Nature of Control and Supervision Authorities'	'Supervisory authority' — an independen t 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

of Personal	e with the	pursuant to	data is	
ce. Data	provisions	Article 51.	processed in	า
regarding	of this		compliance	
	Conventio		with the	
authorities	n.		provisions o	f
and			this	
transborder			Supplement	:ar
data flows:			y Act.	
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			y Act.	
	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	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	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	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

Key principles				and in this Protocol.						
Principles:	Principle of	7. There	Collection	Article 5:	Article 5:	15. Loyalty	Article 13,	Article	Principle of	Article 24:
Fairness	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	should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriat e, with the knowledg e or consent of	limitation principle – Informatio n should be obtained by lawful and fair means, and where appropriat e, with notice to, or consent of, the individual concerned.	Quality of data – Personal data shall be obtained and processed fairly and lawfully.	Legitimac y 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	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 discriminatio n against	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.	5(1)(a): Lawfulness, fairness and transparenc y principle - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.	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.	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.	the data subject.			rights and freedoms at stake. Personal data undergoin	holders shall be considered unfair.				
	Processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.				g processing shall be processed fairly and in a transpare nt manner.					
Principles: Lawfulness (including legal/lawfu I 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 — informatio n should be obtained by lawful and fair means, and where appropriat e, with notice to, or consent of, the	Article 5: Quality of data – Personal data shall be obtained and processed fairly and lawfully.	Article 5: Legitimac y of data processing and quality of data — Personal data undergoin g 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 transparenc y 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	means	individual	processed	compliance	has given	transparent	contrary to	when the
conformity	and,	concerned.	lawfully.	with court	his/her	manner in	the purposes	processing is
with the	where			order,	consent, or	relation to	and	necessary:
purposes and	appropriat		Article 5.2	resolution,	where the	the data	principles of	
principles of	e, with the		Each Party	competent	processing is	subject.	the Charter	- to comply
the Universal	knowledg		shall	public	necessary	Autiala C	of the United	with a legal
Doolovetien of	e or		provide	authority	for:	Article 6	Nations.	obligation
Declaration of	consent of		that data	mandate	- controller's	sets out		- for
Human Rights and the	the data		processing	- necessary	compliance	specific bases for		implementatio
International	subject.		can be	for exercise	with a legal			n of a public
Covenant on			carried	of public	obligation	processing, one of		interest
Civil and			out on the	authority	Obligation	which must		mission or
Political			basis of	powers	-	apply if		relevant to
Rights			the free,	powers	performance	processing		the exercise of
			specific,	- necessary	of a task	is to be		public
Processing of			informed	for defence	carried out in	lawful.		authority
personal data			and	of holder's	the public	Lawful		vested in the
that gives rise			unambigu	rights before	interest, or in	bases		controller
to unlawful or			ous	a public	the exercise	include		- for
arbitrary			consent of	authority	of official	consent of		performance
discrimination			the data	- necessary	authority	the data		of a contract
against the			subject or	for	vested in the	subject,		to which the
data subject			of some	agreement/	controller or	necessary		data subject is
shall be			other	pre-	a third party	for		party or for
deemed unfair.			legitimate basis laid	agreement	-	performanc		the
umair.				_	performance	e of a		application of
Processing of			down by law.	- necessary	of a contract	contract to		pre-
personal data			iaw.	for	to which the	which the		contractual
is necessary				compliance	data subject	data subject		measures at
for the				with a legal obligation	is party, or to	is party,		their request
maintenance				Obligation	take steps at	necessary		

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		- 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 nonfraudulent manner.
--	---	--	--

						freedoms. Public authorities' treatment of personal data is subject to powers granted to them by law.				
Principles: Purpose specificatio n	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 specificati on principle – specified and limited to the fulfilment of those purposes or such others as are not incompati ble with those purposes.	Uses of personal informatio n 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 incompatibl e with those purposes.	Article 5: Legitimac y of data processing and quality of data — Personal data undergoin g 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 incompatibl e 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	in a way	with those	of the person
unambiguous	incompati	purposes.	concerned, in
consent of the	ble with	' '	order to
data subject is	those		make it
given.	purposes.		possible
			subsequently
Principle of			to ensure
Legitimacy:			that:
Personal data			
can be			(a) All the
processed a.			personal data
after			collected and
obtaining the			recorded
free,			remain
unambiguous			relevant and
and informed			adequate to
consent of the			the purposes
data subject;			so specified;
b. where a			(b) None of
legitimate			the said
interest of the			personal data
responsible			is used or
person			disclosed,
justifies the			except with
processing			the consent
and the			of the person
legitimate			concerned,
interests,			for purposes
rights and			incompatible
freedoms of			with those
data subjects			specified;
uata subjects			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: Proportion ality	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 informatio n 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: Legitimac y of data processing and quality of data — Data processing shall be proportio nate in relation to the legitimate purposes pursued	18. Proportionali ty 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 minimisatio n 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 datashall be adequate and relevant in relation to the purposes for which it is collected and further processed.

Processed	approp-	for which	and reflect	they are	for which	certain
personal data	riate, with	they are	at all	collected and	they are	amount of
limited to the	the know-	stored.	stages a	further	processed.	publicity or
minimum	ledge or		fair	processed.		be brought to
necessary.	consent of		balance			the attention
	the data		between			of the person
	subject.		all			concerned, in
	Personal		interests			order to
			concerned			make it
	data should be		, whether			possible
	relevant		public or			subsequently
	to the		private,			to ensure
			and the			that:
	purposes for which		rights and			(a) All the
	they are		freedoms			personal data
	to be		at stake.			collected and
	used.		Personal			recorded
	uscu.		data			remain
			under-			relevant and
			going			adequate to
			processing			the purposes
			shall be			so specified.
			adequate,			30 Specifica.
			relevant			
			and not			
			excessive			
			in relation			
			to the			
			purposes			
			for which			

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,	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 informatio n principle –  Personal informatio n 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 identificatio n of the data subjects for no longer than is required for the purpose	they are processed.  Article 5: Legitimac y of data processing and quality of data — Personal data undergoin g processing shall be accurate and, where necessary, kept up to date and preserved in a form which permits	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	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	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	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
	limited to the minimum	up-to-		than is required for	in a form which		incomplete, having regard	regard to the	that they are kept as	obtained and further

	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 / transparen cy  + 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 developments, 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  Exemption s: - 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: Legitimac y of data processing and quality of data — Personal data under- going processing shall be processed fairly and in a transpare nt manner	16. Transparenc y principle — The person responsible shall inform the holder about the existence and main characteristic s 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 transparenc y 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	ing the	informatio	habitual	Article 8:	controller	the attention	whose
intended	existence	n	residence	Transpare	shall provide	of the person	personal data
purpose of	and	identifying	or principal	ncy of	the natural	concerned.	is being
processing,	nature of	an	place of	processing	person		processed
the recipients	personal	individual	business of	_	whose data		with
to whom their	data, and	in their professiona	the	controller	are to be		information
personal data	the main	I capacity.	controller	to inform	processed		on its identity,
will be	purposes	r capacity.	of the file.	data	with		purposes,
disclosed and	of their			subjects of	information		recipients,
how data	use, as			identity,	on its		existence of
subjects may	well as the			habitual	identity,		certain rights,
exercise these	identity			residence	purposes,		the
rights and	and usual			or	categories of		preservation
further	residence			establishm	data,		period, and
information	of the			ent; legal	recipients,		possibility of
necessary to	data			basis and	existence of		transfer to a
guarantee fair	controller.			purposes	certain		third country.
processing of				of	rights,		
such data.				processing	storage		
When				, the	period, and		
personal data				categories	proposed		
have been				of	transfers to		
collected				personal	third		
directly from				data	countries.		
the data				processed,			
subject, the				recipients,			
information				or			
must be				categories			
provided at				of			
the time of				recipients,			
collection,				the means			
				of			

-1	an alwandi.				1
	ss already	exercising			
provi	ided.	data			
Whe	n	subject's			
	onal data	rights			
•		Formutia			
	not been	Exemptio			
colle		n			
	tly from	Article 11:			
the d		Exception			
_	ect, the	s and			
respo	onsible	restriction			
•	on must	s – when			
also i	inform	such an			
him/	her				
abou	it the	exception			
sourc	ce of	is			
perso	onal data,	provided			
withi		for by law,			
reasc	onable	respects			
perio	od of time	the			
	may be	essence of			
	aced by	the			
	native	fundamen			
	sures if	tal rights			
		and			
	oliance is	freedoms			
	ossible or	and			
	d involve	constitute			
a		s a			
	roportion	necessary			
	effort by	and			
the		proportio			
		nate			
		liate	1		ĺ

responsible	measure
person.	in a
Any information to be furnished to the data subject in an intelligible form, using clear and plain language, in particular for any processing	in a democrati c society for:  - protection of national security, defence, public safety, important economic and financial
addressed specifically to minors.  When personal data is collected online, by means of electronic communicatio ns networks, the obligations set out above may be	interests of the State, the impartialit y and independe nce of the judiciary or the preventio n, investigati on and prosecutio n of

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

	for by law	$\overline{}$
	with	
	respect to	
	data	
	processing	
	for	
	archiving	
	purposes	
	in the	
	public	
	interest,	
	scientific	
	or	
	historical	
	research	
	purposes	
	or	
	statistical	
	purposes	
	where	
	there is no	
	recognisa	
	ble risk of	
	infringem	
	ent of the	
	rights and	
	fundamen	
	tal	
	freedoms	
	of data	
	subjects.	

Principles:	Accountabilit	14. A data	Accountabi	Article 10:	20.	Article 5(2):	
	y principle –	controller	lity	Additional	Responsibilit	Accountabil	
Accountabi		should be	principle –	obligation	y principle –	ity principle	
lity	The	account-	controller	<b>s</b> – each	The person	– The	
	responsible	able for	should be	Party shall	responsible	controller	
	person shall	complying	account-	provide	shall	shall be	
	take all	with	able for	that	implement	responsible	
	necessary	measures	complying with	Contr-	necessary	for, and be	
	measures to	which give	measures	ollers and,	mechanisms	able to	
	observe the	effect to	that give	where	to prove	demonstrat	
	principles and	the	effect to	applicable,	compliance,	e	
	obligations	principles	the	processors	shall be	compliance	
	set out in this	stated	principles.	, take all	accountable	with,	
	Resolution	above.	When	approp-	to the holder	paragraph 1	
	and in the	45 A data	inform-	riate	and to the	[the	
	applicable	15. A data	ation is	measures	control	principles]	
	national	controller	transferred to another,	to comply	authority.	Autista 24.	
	legislation	should:	the	with the	N. A. a. la a. u. i a. u. a	Article 24:	
	and have the	a) Have in	controller	obligat-	Mechanisms	Responsibili	
	necessary	place a	should	ions of	to adopt may		
	internal	privacy	obtain	this	be:	controller -	
	mechanism in	managem	consent or	Convent-	- data	The	
	place for	ent	exercise	ion and be	protection	controller	
	demonstratin	programm	due	able to	programs	shall	
	g such	e and be	diligence,	demon-	and policies	implement	
	observance	prepared	taking	strate that		appropriate	
	both to data	to demon-	reasonable	the data	- risk	technical	
	subjects and to the	strate the	steps to ensure that	processing	management	and	
		prog-	the	under	systems	organisatio	
	supervisory authorities in	ramme as	recipient	their	- training	nal	
	the exercise	approp-	will protect	control is		measures	
	the exercise	riate, in	the	in		to ensure	

	of their powers as established under section on Compliance and monitoring:	particular at the request of a competen t privacy enforcem ent	informatio n in line with the principles.		complianc e.	<ul><li>reviews of policies and programs</li><li>audits</li><li>complaints procedures.</li></ul>		and to be able to demonstrat e that processing is performed in		
	Independent Supervisory authorities powers and competences.	authority or another entity responsibl e for promoting adherence to a code of conduct or similar arrangem ent giving binding effect to these Guidelines						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 – appropriat e 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 confidentialit y and security of	Article 5(1)(f): Integrity and confidential ity principle	Principle of security – Appropriate measures should be taken to	Article 28: Principle of confidentialit y and security - Personal data shall be

protect the personal data safeguards subject to processing with the appropriate technical and organizational measures to ensure, at each time, tonflichentiality and availability.  **Processing with the appropriate technical and organizational measures to ensure, at each time, tonflichentiality and availability.  **Processing with the appropriate technical and organizational measures to ensure, at each time, the integrity, confidentiality and availability.  **Processing with the appropriate technical and organizational measures to ensure, at each time, the integrity, confidentiality and availability.  **Processing the processor of takes and where appropriate to data stored in takes and where appropriate the processor in takes and technical processor in the guarantee to execurity and as against unauthorised accidental loss as well as a saginst unauthorised accidental loss as well as against unauthorised accidental loss as well as accidental loss, suse, alteration or disclosure of integrity.  **Processing berosnal data and technical processor in the guarantee to execurity and any availability of a data.  **Processing the processing and technical processing and processing and processing and processing and processing and processing and them as a security of the data over a unauthorise of the data over a unauthorise of the data.  **Processing the procession and technical processing and the ensures the processing and the p	n	rovider must	reasonabl	loss/	shall be	that the	maintain	personal	– Personal	protect the	processed
personal data subject to processing with the appropriate technical and organizational measures to ensure, at each time, their integrity, and availability.  The integrity and availability.  A validability.  Define the processing with the appropriate technical and availability.  Define the processing with the appropriate technical and availability.  Define the processing with the appropriate technical and availability.  Define the processing the processor, modification or dissemination.  Define the processing that as tored data stored data stored disclosure. A cidental loss or within the processing that a processed confidentially against as accidental loss or within the processing that a processed confidentially or processing and appropriate the processing that any processing t	•			-				•		· .	_ ·
subject to processing such risks with the proper proper proper technical and organizational measures to ensure, at each time, their integrity, and availability.  **Total Controller shape of the data or access, alteration or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or dissemination.**  **Total Controller shape of the data or access, alteration or or or dissemination.**  **Total Controller shape of the data or access to, alteration or or or dissemination.**  **Total Controller shape of the data or access to, alteration or or dissemination.**  **Total Controller shape of the data or access to, alteration or or dissemination.**  **Total Controller shape of the data or access to, alteration or or dissemination.**  **Total Controller shape of the data or access to, alteration or or dissemination.**  **Total Controller shape of the data or access to, alteration or or dissemination.**  **Total Controller shape of the data or and against and against accidental loss, alteration or disclosure of the data.**  **Total Controller shape of the data or and technical or and technical or one disclosure of the data or and availability of accessing and against accidental loss, alteration or disclosure of data.**  **Total Controller shape of the data or and processing and against and against and against accidental loss, alteration or disclosure of data.**  **Total Controller shape of the data or and technical shall be measures in order to confidentially and and technical shall be measures in order to confidentially and and technical shall be measures in order to confidentially and and technical shall be processed that the data or or and t	•		•			,				•	,
processing with the as loss or appropriate technical and organizational measures to ensure, at each time, or their integrity, confidentiality and availability.  **Total Controllers against the masures in or discoure availability.**  **Total Controllers against to as against and technical and organizational and availability.**  **Total Controllers against the measures in order to appropriate takes adainst takes and technical and data stored takes and technical and destruction and availability.**  **Total Controllers against the measures in order to appropriate and technical and technical and technical and technical and technical and availability.**  **Total Controllers against the measures in order to appropriate takes adainst takes and technical an	•		_								
with the apropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability.  With the apropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability.  A validability.  We have the processed order to guarantee accidental or unauthorised accidental loss as well accidental loss as well access, alteration or or dissemination.  We have the confidentially of data.  When processed confidentially and appropriate accidental or unauthorise data or unauthorise data.  When processing in measures in order to guarantee appropriate against and alteration or dissed accidental loss as well accidental loss as well access, alteration or disclosure ination.  When processed confidentially and appropriate accidental or unauthorise data.  When the appropriate takes confidentially appropriate against and arcidental or unauthorise of data.  When the appropriate takes confidentially appropriate against and arcidental or unauthorise of data.  When destruction appropriate against and arcidental or or discource of the data or unauthorise of the data over a network.  Controllers and aprocessing involved integrity and accidental loss are well access to, access, alteration or disclosure of destruction or disclosure of the data or unauthorise of destruction or disclosure of the data or unauthorise or derived and processing appropriate to the personal data.  Controllers and against against and availability of the data or unauthorise of the data or unauthorise or destruction or disclosure or disclosure of the data or unauthorise or destruction or disclosure or di		-	_		•			•	•	•	'
appropriate technical and organizational measures to ensure, at each time, their integrity, and availability.  In automated data files against each time, their integrity, and availability.  In automated data files against on or or discomenination.  In automated data files against measures against or unauth-orised availability of destruction or discomenination.  In automated data files appropriate escurity gard accidental or unauth-orised availability of destruction or discomenination.  In automated data files appropriate escurity of gardicular where the personal data, availability of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing availability of data.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing availability of a protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Controllers and processing involved including protection of the data over a network.  Cont	•	_		destruction	·						•
technical and organizational measures to nensure, at each time, their integrity, confidentiality and availability.  In the integrity of disclosure and availability.  In the integrity of disclosure and availability.  In the integrity of disclosure accidental or or unauth-accidental loss as well as against unauth-orised access to, alteration or dissemination.  In the where the personal data, including transmission of data or or or unauth-orised adata, including transmission of the data or over a unauthorise of dor unauth-orised adainst accidental loss, ase, modification or or dissemination.  In the where the personal data, including transmission of the data or over a unauthorise of the data or over a unauthorise of dor unauth-orised against accidental or or darage, unauthorise of dor unauthoris				, use,		•		•			
organizational measures to ensure, at each time, their integrity, and availability.  Confidentiality and availability.  Of data.  Article 21:  Organizational measures to ensure, at each time, their integrity, and availability.  Organizational measures to ensure, at each time, their integrity, and availability.  Organizational measures to ensure, at each time, their integrity, and availability.  Organizational measures to ensure, at each time, their integrity, and availability of disclosure of data.  Organizational measures to ensure, at each time, their integrity, and availability of destruction or disclosure of data.  Organizational measures to ensure, at each time, their integrity, and availability of destruction or access to, as against unauth-orised access to, alteration or discoure ination.  Organizational measures to ensure, at each time, their integrity, and availability of data.  Or disclosure of data.  Or data or ounauth-orised or unauthorized availability of of the data or controllers and processors must ensure compliance with security measures defined in this conversion.  Organizational measures to ensure that it is not deformed, damaged or accessible to a data or or unauthorized availability of the data, and in particular the personal data, including transmission of the data, availability of the data, availability of the data, availability of the data, and in particular to ensure that it is not deformed, damaged or access to, alteration or disclosure of the data.  Organization or unauth-orised access to, destruction or disclosure of the data.  Organization or unauth-orise of the data or controller viruses.  Obligations of controller viruses.  Obligations of or ontroller viruses.  Obligations of or ont	•			modificatio				· .			
measures to ensure, at each time, their integrity, confidentiality and availability.  In measures to ensure, at each time, their integrity, confidentiality and availability.  In measures to ensure, at each time, their integrity, confidentiality and availability.  In the personal data, including processing availability of destruction or unauthorised as against unauthorised access, alteration or dissemination.  In the personal data, including processing and against unauthorise and processing and against unauthorise and processors must ensure compliance with security measures defined in this Convention.  In the personal data, including processing and against unauthorise and processing and against accidental loss, use, modification or dissemination.  In the personal data, including processing and against unauthorise and processing and against accidental loss, destruction or data, and in particular to ensure that it is not deformed, damaged or accessible to			· ·	n,			•				
ensure, at each time, their integrity, confidentiality and availability.  In the integrity of data.  In the integrity of data or or data or or data or or data or or or dissemination.  In the integrity of data or or of the data or over a unauthorise of the data or or or data or or on the data or over a unauthorise of and against or or or data or or on the data or or or or data or or or or data or or data or or data or or or data or or or data or or or data or or or data		_		disclosure.		•		' '	•	_	
each time, their integrity, confidentiality and availability.  I and availability of personal data.  I and availability of data availability of of data availability of personal data.  I and availability of data.  I and availabili					_			•	the		
their integrity, confidentiality and availability.  or destruction or accidental loss as well as against unauth-orised access, alteration or or dissemination.  or disclosure of data.  or unauth-orised access, alteration or or dissemination.  or discention or or dissemination.  or accidental loss as well as against unauth-orised access, alteration or or dissemination.  or discention or accidental loss, use, modifination.  or discention or discention or or dissemination.  or accidental loss as well as against unauth-orised access, alteration or or dissemination.  or accidental loss as well as access to, as against unauth-orised access, alteration or or dissemination.  or accidental loss as well as access to, as against unauth-orised access, alteration or or dissemination.  or accidental loss as well as access to, as against unauth-orised access, alteration or or dissemination.  or accidental loss as well as access to, as against unauth-orised access, alteration or or dissemination.  or accidental loss as well as access to, as against unauth-orise network.  Ontrollers and processing and against accidental over a unlawful processing and against accidental loss, destruction or damage, using appropriate technical or or organisatio or data, and in particular to ensure that it is not deformed, damaged or accessible to		•				_	• • • • • • • • • • • • • • • • • • • •		•	unauthorized	network.
destruction or unauth- orised as against unauth- orised as against unauth- oridised access, alteration or dissemination.    Controllers and processors must ensure compliance ination.   Article 21: Security   Market   Ma		•				risks such		ı ·	•	·	
and availability.  or accidental loss as well as against unauth-orised access to, dest-unauth-orised access, alteration or dissemination.  or unauth-orised access, alteration or dissemination.  of the data over a unauthorise over a network.  Controllers and processors must ensure compliance with security measures defined in this Convention.  Article 21: Security  of the data over a unauthorise dor unauthorise of or contaminatio n by computer viruses.  Obligations of security – the data over a unauthorise of or ontaminatio n by computer viruses.  Obligations of security – the data over a unauthorise of or unauthorise of or ontaminatio n processing and against accidental loss, security of measures defined in this Convention.  Article 21: Security  Adata or Obligations of security – the data over a unauthorise of or ontaminatio n by computer viruses.  Security – the data over a unauthorise of or ontaminatio n by computer viruses.  Security – the data or controller viruses.  Article 21: Security  Mata or Obligations of security – the data over a unauthorise of or ontaminatio n by computer viruses.  Security – the data over a unauthorise of or ontaminatio n by computer viruses.  Security – the data or or ontaminatio or on data against and against accidental loss.  Article 21: Security					orised		l -		including		
availability.  accidental loss as well as against unauth- orised access, alteration or dissemination.  accidental loss as well as against unauth- orised access, alteration or disclosure ination.  accidental loss as well access to, destruction, orised access, alteration or disclosure of personal data.  accidental loss as well access to, destruction, orised access, alteration or disclosure of personal data.  accidental loss as well access to, destruction or disclosure of personal data.  accidental loss as well access to, destruction or disclosure of personal data.  accidental loss, use, modif-ication or disclosure of personal data.  access to, destruction or destruction or damage, using appropriate technical or organisatio nal measures.  accidental or on by computer viruses.  accidental loss, destruction or damage, using appropriate technical or organisatio nal measures.  accidental loss, destruction or damage, using appropriate technical or organisatio nal measures.	CC	onfidentiality	of data.		destruction	accidental	personal	transmission	protection	misuse of	Article 43:
loss as well as against unauth- orised access, alteration or dissemination.  Ioss as well as against unauth- orised access, alteration or dissemination.  Ioss, use, modification or of disclosure ination.  Ioss, use, modification or of disclosure ination.  Ioss, use, modification or disclosure ination.  Ioss, use, modification or disclosure of personal data.  Ioss, destruction or damage, using appropriate technical or organisatio  Article 21:  Security  In by computer viruses.  In by computer	aı	nd			or	or unauth-	data.	of the data	against	data or	Obligations of
as against unauth- orised access, alteration or dissemination.  of personal data.  as against unauth- orised access, alteration or dissemination.  as against unauth- orised access, alteration or dissemination.  as against unauth- ruction, loss, use, modification or disclosure of personal data.  Controllers and processing and against accidental loss, destruction or damage, using appropriate technical or or ganisatio appropriate technical or or organisatio appropriate technical or or organisatio and against accidental loss, destruction or damage, using appropriate technical or or organisatio appropriate technical or or organisatio and against accidental loss, destruction or damage, using appropriate technical or or organisatio appropriate technical organisation appropriate technical	a	vailability.			accidental	orised		over a	unauthorise	contaminatio	security – the
unauth- orised access, alteration or dissem- ination.  unauth- orised access, alteration or dissem- ination.  unauth- orised access, alteration or dissem- ination.  disclosure of personal data.  accessing and processing and against accidental loss, destruction or damage, using appropriate technical or organisatio Article 21: Security measures.  defined in this Convention.  Article 21: Security  processing and against accidental loss, destruction or damage, using appropriate technical or organisatio deformed, damaged or accessible to					loss as well	access to,		network.	d or	n by	data
unauth- orised access, alteration or dissemination.  Ination.  Ina					as against	dest-		Controllors	unlawful	computer	controller
orised access, alteration or dissemination.  of personal data.  orised access, alteration or dissemination.  of personal data.  of data, and in particular to ensure that it is not or organisatio deformed, damaged or accessible to					unauth-	ruction,			processing	viruses.	shall take all
access, alteration or dissemination.  Indication or dissemination.  Indication or disclosure of personal data.  Indication or disclosure of personal data.  Indication or disclosure of personal data.  Indication or disclosure of disclosure of personal data.  Indication or disclosure of disclosure of personal data, and in particular to ensure that it is not organisatio organisatio deformed, damaged or accessible to					orised	loss, use,			and against		necessary
alteration or dissemination.  or dissemination.  of personal data.  alteration or dissemination.  of personal data.  compliance with security measures defined in this Convention.  Article 21: Security  not disclosure of data, and in particular to ensure that it technical or or ganisatio deformed, damaged or accessible to					access,	modif-		•	accidental		precautions in
of discours ination.  of personal data.  with security measures defined in this Convention.  Article 21: Security measures.  of data, and in particular to ensure that it is not deformed, damaged or accessible to					alteration	ication or			loss,		relation to the
Ination.  Of personal data.  Measures defined in this Convention.  Article 21:  Security  Or damage, using appropriate technical or organisatio nal damaged or accessible to					or dissem-	disclosure		I	destruction		nature of
personal data.  personal data.  personal data.  personal data.  personal data.  personal data.  lefined in this Convention.  Article 21: Security measures.  particular to ensure that it is not deformed, damaged or accessible to					ination.	of		,	or damage,		data, and in
this convention.  Article 21: Security  This technical or organisatio appropriate technical or organisatio deformed, damaged or accessible to						personal			using		
Convention.  Convention.  Convention.  Convention.  Convention.  Article 21: Security  Technical or organisatio deformed, damaged or accessible to						data.			appropriate		ensure that it
Article 21: nal deformed, damaged or security measures. deformed, damaged or accessible to									technical or		is not
Article 21: nal damaged or accessible to								Convention.	organisatio		deformed,
Security measures. accessible to								Article 21:	nal		•
									measures.		_
ODIIgations –								obligations –			
the data								_			

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

						appropriate technical and organisatio nal 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	Article 5: Quality of data – Personal data shall be preserved in a form which permits identificatio n of the data subjects for no longer than is required for the purpose for which	Article 5: Legitimac y of data processing and quality of data — Personal data undergoin g processing shall be preserved in a form which permits identificati on of data	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	Article 5(1)(e): Storage limitation principle - Personal data shall be kept in a form which permits identificatio n of data subjects for no longer than is necessary for the purposes for which	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	Article 25: Principle of purpose, relevance and preservation — Personal datashall be kept for a period which shall not exceed the period required for the purposes for which they were obtained and processed. Beyond the

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

Data subject rights								and organisatio nal measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.		
Data	Right of	13.	Access and	Article 8:	Article 9:	25. Right to	Article 17:	Article 15:	Principle of	Article 39:
subject	access –	Individuals	Correction	Additional	Rights of	Access –	Right of	Right of	interested	Right of
rights:		should	principle –	safeguards	the data	Holder shall	access –	access by	person	access – an
	Data subject	have the	individuals	for the data	subject –	have the	Natural	the data	access –	individual
Access	has the right	right:	should be	subject –	Every	right to	persons	subject –	Everyone	whose
	upon request	2) +0	able to obtain	Any person	individual	request	whose data	The data	who offers	personal data
	to obtain information	a) to obtain	confirmatio	shall be	shall have	access to its	are to be	subject	proof of	is the subject
+ Examplians	on the	from a	n of	enabled to	the right	personal data	processed	shall have	identity has	of processing
Exemptions	specific	data	processing	obtain ()	to obtain,	in possession	can request	the right to	the right to	may request
	personal data	controller,	and to have	confirmatio	on request	of the	information	obtain from	know	information to
	P = 1 = 2 = 1 = 1	33.12.31121,	the	n of	()		to enable	the	whether	enable them

	T	1 _		T					1
subject to	or	informatio	whether	confirmati	responsible	them to	controller	information	to be
processing, as	otherwise,	n .	personal	on of the	person.	evaluate the	confirmatio	concerning	informed of
well as the	confirmati	communica	data are	processing		processing,	n as to	him is being	and contest
source of such	on of	ted to them	stored as	,		confirmation	whether or	processed	the
data, the	whether	them	well as	communic	Exemptions:	as to	not	and to obtain	processing,
purposes of	or not the		communica	ation in an	Notional	whether data	personal	it in an	confirmation
processing	data	Exemption	tion to him	intelligible	National	are being	data	intelligible	as to whether
and the	controller	s:	of such data	form of	legislation	processed,	concerning	form,	data are being
recipients or	has data	3.	in an	the data	shall	the data	him or her	without	processed,
categories of	relating to	-	intelligible	processed.	establish, but	being	are being	undue delay	disclosure of
recipients to	them;	unreasona	form.		could be:	processed	processed,	or expense,	the data being
whom such	h) + a h a a	ble or			- treatment	and any	access to	and to have	processed and
data are or	b) to have communic	disproporti		Exception	necessary for	information	the	appropriate	any
will be	ated to	onate burden or	Exemptions	s,	compliance	as to its	personal	rectifications	information as
disclosed.	them,	expense		restriction	with an	source, the	data and	or erasures	to its origin,
Information	data		Article 9:	s:	important	purpose of	information	made in the	the purpose of
to the data	relating to	- legal or	- when such		purpose of	processing	about	case of	processing
subject must	them	security	derogation	Exemptio	public	and	purposes of	unlawful,	and recipients.
be provided in	tileili	reasons, or	is provided	ns:	interest	recipients.	the	unnecessary	
an intelligible	i. within a	commercial confidentia	for by the	Article 11:			processing;	or inaccurate	
form, clear	reasonabl	lity	law of the	Exception	- treatment		categories	entries and,	
and simple	e time;	iity	Party and	s and	necessary for		of personal	when it is	
language.		- violation	constitutes	restriction	exercising		data;	being	
The	ii. at a	of other	a necessary	s – when	the functions		recipients	communicate	
_	charge, if	individuals'	measure in	such an	of public		or	d, to be	
responsible	any, that	informatio	а	exception	authorities		categories	informed of	
person must	is not	n privacy.	democratic	is	- person		of recipient;	the	
implement	excessive;		society in	provided	responsible's		retention	addressees.	
procedures to	iii. in a		the	for by law,	legitimate		period or	Provision	
enable this	reasonabl		interests of:	respects	motives		criteria	should be	
right to be				the	prevail over		used to	made for a	
exercised in a				essence of	holder's		determine	remedy, if	
		1			ווטוענו ז			•	

simple, fast	e manner;	- protecting	the	interests,	it; the	need be with	
and efficient		state	fundamen	rights and	existence of	the	
way, with no	st	security;	tal rights	freedoms	other data	supervisory	
undue delay	iv. in a	public	and		subject	authority	
or cost of ga	in   form that	safety;	freedoms	- treatment	rights;	specified in	
for the	is readily	monetary	and	necessary for	information	principle 8. It	
responsible	intelligible	interests of	constitute	compliance	as to the	is desirable	
person. The	to them;	state or the	s a	with a legal	source of	that the	
data subject	c) to be	suppression	necessary	obligation	the data;	provisions of	
must be	given	of criminal	and	- personal	the	this principle	
informed of	reasons if	offences	proportio	data	existence of	should apply	
the reasons,			nate	necessary for	automated	to everyone,	
the exercise	made	- protecting	measure	maintenance	decision-	irrespective	
of this right	under	the data	in a	or	making,	of nationality	
under	subparagr	subject and	democrati	compliance	including	or place of	
applicable	aphs (a)	the rights	c society	with a legal	profiling,	residence.	
national	and (b) is	and freedoms of	for:	or	and		
legislations	s denied,			contractual	information		
not justified	and to be	others	protection	relation.	about the	Exemptions:	
	able to	-	of national		logic	Firesutions	
	challenge	Restrictions	security,		involved; if	Exceptions	
Exemptions	such	may be	defence,		data is	authorized only as	
National	denial;	provided by	public		transferred		
legislation	and	law with	safety,		to a third	necessary to protect	
may limit	d) to	respect to	important		country or	national	
repetitive	challenge	data used	economic		internation	security,	
exercise of	data	for statistics	and		al	public order,	
this right	relating to	or scientific	financial		organisatio	public health	
when	them and,	research	interests		n,	or morality,	
responding	· · · · · · · · · · · · · · · · · · ·	purposes	of the		information	as well as,	
multiple	challenge	and where	State, the		about	inter alia, the	
martiple	- Indirecting -	there is	1111, 3113		safeguards;	cci alia, tile	

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

Г	T	1	1	
	tal			
	freedoms			
	of others,			
	notably			
	freedom			
	of			
	expression			
	CAPT COSTON			
	'			
	Restriction			
	s 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			
1		<u> </u>	1	

			there is no recognisa ble risk of infringem ent of the rights and fundamen tal 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	shall have a right to object at any time () to the processing of	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	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,	provisions	controller	including	relating to	on certain	relating to
satisfactorily	of domestic	demonstr	profiling.	them is	lawful	them is
establishing	law giving	ates		disclosed for	bases.	disclosed for
his/her	effect to	legitimate		the first time		the first time
identity, or	the basic	grounds	Exemptions:	to third	The right to	to third
through a	principles	for the		parties, or	object	parties, or
representativ	set out in	processing	National	used for	applies at	used on behalf
e,	Articles 5	which	legislation	marketing,	any time when	of a third
satisfactorily	and 6 of	override	shall	and to be		party for
establishing	this	his or her	establish, but	offered the	processing is for the	marketing,
his/her	Convention.	interests	could be:	right to	purposes of	and to be
identity.		or rights	- treatment	object to	direct	offered the
The		and	necessary for	those	marketing.	right to object
responsible		fundamen	compliance	disclosures/	marketing.	to those
person must		tal	with an	uses.		disclosures/
implement		freedoms.	important			uses.
procedures to			purpose of			
enable this			public			
right to be		Exemptio	interest			
exercised in a		ns:	- treatment			
simple, fast		Article 11:	necessary for			
and efficient		Exception	exercising			
way, with not		s and	the functions			
undue delay		restriction	of public			
or cost of gain		s – when	authorities			
for the		such an				
responsible		exception	- the person			
person. The		is	responsible's			
data subject		provided	legitimate			
must be		for by law,	motives			
informed of		respects	prevail over			
		·	holder's			

l t	the reasons, if	the	interests,
	the exercise	essence of	rights and
	of this right	the	freedoms
	under	fundamen	incedoms
	applicable	tal rights	- treatment
	national	and	necessary for
	legislations is	freedoms	compliance
	not justified.	and	with a legal
'	not justificu.	constitute	obligation
		s a	norconal
	Framentians	necessary	- personal data
	Exemptions:	and	
7	The exercise	proportio	necessary for maintenance
	of this right is	nate	
r	not justified	measure	or
\	where the	in a	compliance
	processing is	democrati	with a legal or
r	necessary for	c society	contractual
t	the	for:	relation.
	performance	101.	relation.
	of a duty	-	
i	imposed on	protection	
t	the	of national	
r	responsible	security,	
	person by the	defence,	
á	applicable	public	
r	national	safety,	
I	legislation.	important	
_	The data	economic	
	The data	and	
	subject may	financial	
	also object to	interests	
t	those		

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

viewpoint in	and
order to	fundamen
defend	tal
his/her	freedoms
right/interest.	of others,
	notably
	freedom
	of
	expression
	Restriction
	s 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 recognisa ble risk of infringem ent of the rights and fundamen tal freedoms of data subjects.					
Data subject rights:  Rectificatio n  + 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, confirmati on of whether or not the data controller	Access and Correction principle – individuals should be able to challenge the accuracy of personal informatio n, and if possible and as appropriat e have the informatio n 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 () rectificatio n 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 rectificatio n – 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

	Τ		Ι.	l .a .		T	_		
responsible	has data	amended	the	if these		where such	concerning	form,	subject is
person should	relating to	or deleted.	provisions	are being,	Exemptions:	data are	him or her.	without	entitled to ask
carry out the	them;		of domestic	or have	Exemptions.	inaccurate,	Taking into	undue delay	the controller
rectification	b) to have	_	law giving	been,		incomplete,	account the	or expense,	to have the
and notify	communic	Exemption	effect to	processed	Niational	equivocal or	purposes of	and to have	data rectified,
third parties	ated to	s:	the basic	contrary	National	out of date,	the	appropriate	supplemented
to whom	them,	-	principles	to the	legislation	or whose	processing,	rectifications	, updated,
personal data	data	unreasona	set out in	provisions	shall	collection,	the data	or erasures	blocked or
has been	relating to	ble or	Articles 5	of this	establish, but	use,	subject	made in the	destroyed as
disclosed, if	them	disproporti	and 6	Conventio	could be:	disclosure or	shall have	case of	appropriate.
known.	tileili	onate	(Quality of	n.	- treatment	storage are	the right to	unlawful,	
The	i. within a	burden or	data,		necessary for	prohibited.	have	unnecessary	
	reasonabl	expense	special		compliance		incomplete	or inaccurate	
responsible	e time;	- legal or	categories	Exception	with an		personal	entries and,	
person must		security	of data)	s and	important		data	when it is	
implement procedures to	ii. at a	reasons, or		restriction	purpose of		completed,	being	
enable this	charge, if	commercial		s:	public		including by	communicate	
	any, that	confidentia	Exceptions		interest		means of	d, to be	
right to be exercised in a	is not	lity	and	Article 11:			providing a	informed of	
simple, fast	excessive;	- violation	restrictions:	Exception	- treatment		supplement	the	
and efficient	iii. in a	of other		s and	necessary for		ary	addressees.	
	reasonabl	individuals'	Article 9:	restriction	exercising		statement.	Provision	
way, with not	e manner;	informatio	- when such	s – when	the functions		Autiolo 10.	should be	
undue delay or cost of gain	and	n privacy.	derogation	such an	of public		Article 19: Notification	made for a	
			is provided	exception	authorities			remedy, if	
for the	iv. in a		for by the	is	- the person		obligation -	need be with	
responsible	form that		law of the	provided	responsible's		controller shall	the	
person. The	is readily		Party and	for by law,	legitimate			supervisory	
data subject must be	intelligible		constitutes	respects	motives		communica	authority	
	to them;		a necessary	the	prevail over		te any	specified in	
informed of	c) to be		measure in	essence of	holder's		rectification	principle 8.	
the reasons, If	given		а	the	interests,		or erasure	The cost of	
	1 0	l	1			1			

the exercise of this right under applicable national legislations is not justified.	reasons if a request made under subparagr aphs (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	fundamen tal rights and freedoms and constitute s a necessary and proportio nate measure in a democrati c 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 disproporti onate 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,	
---	--	--	--	--	--	--	---	--

		1
or scientific	y and	inter alia, the
research	independe	rights and
purposes	nce of the	freedoms of
and where	judiciary	others,
there is	or the	especially
obviously	preventio	persons
no risk of an	n,	being
infringemen	investigati	persecuted
t of the	on and	(humanitaria
privacy of	prosecutio	n clause)
the data	n of	provided that
subjects.	criminal	such
	offences	departures
	and the	are expressly
	execution	specified in a
	of criminal	law or
	penalties,	equivalent
	and other	regulation
	essential	promulgated
	objectives	in
	of general	accordance
	public	with the
	interest;	internal legal
	and the	system which
	protection	expressly
	of the	states their
	data	limits and
	subject or	sets forth
	the rights	appropriate
	and	safeguards.
	fundamen	
	tal	

freedoms
of others,
notably
freedom
of
expression
Restriction
s 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

					recognisa ble risk of infringem ent of the rights and fundamen tal 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, confirmati on of whether or not the data controller has data	Access and Correction principle – individuals should be able to challenge the accuracy of personal informatio n, and if possible and as appropriat e have the informatio n 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 rectificatio n 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	relating to		of domestic	been,	person	inaccurate,	the	undue delay	the controller
notified,	them;		law giving	processed	responsible	incomplete,	controller	or expense,	to have the
where known.		Exemption	effect to	contrary	to stop	equivocal or	shall have	and to have	data rectified,
	b) to have	s:	the basic	to the	treating	out of date,	the	appropriate	supplemented
The	communic	-	principles	provisions	them.	or whose	obligation	rectifications	, updated,
responsible	ated to	unreasona	set out in	of this	them.	collection,	to erase	or erasures	blocked or
person must	them,	ble or	Articles 5	Conventio		use,	personal	made in the	destroyed as
implement	data	disproporti	and 6	n.	Exemptions:	disclosure or	data	case of	appropriate.
procedures to	relating to	onate	(Quality of	11.	exemptions.	storage are	without	unlawful,	арргорпасс.
enable this	them	burden or	data,		National	prohibited.	undue	unnecessary	
right to be	i. within a	expense	special	Exception	legislation	prombited.	delay where	or inaccurate	
exercised in a	reasonabl	- legal or	categories	s and	shall		certain	entries and,	
simple, fast	e time;	security	of data)	restriction	establish, but		grounds	when it is	
and efficient	c time,	reasons, or	0. 0.0.00,	s:	could be:		apply.	being	
way, with not	ii. at a	commercial			- treatment			communicate	
undue delay	charge, if	confidentia	Exceptions	Article 11:	necessary for		Article 19:	d, to be	
or cost of gain	any, that	lity	and	Exception	compliance		Notification	informed of	
for the	is not	- violation	restrictions:	s and	with an		obligation -	the	
responsible	excessive;	of other		restriction	important		controller	addressees.	
person. The	iii. in a	individuals'	Article 9:	<b>s</b> – when	purpose of		shall	Provision	
data subject	reasonabl	informatio	- when such	such an	public		communica	should be	
must be	e manner;	n privacy.	derogation	exception	interest		te any	made for a	
informed of	and		is provided	is	interest		rectification	remedy, if	
the reasons, if	ana		for by the	provided	- treatment		or erasure	need be with	
the exercise	iv. in a		law of the	for by law,	necessary for		of personal	the	
of this right	form that		Party and	respects	exercising		data or	supervisory	
under	is readily		constitutes	the	the functions		restriction	authority	
applicable	intelligible		a necessary	essence of	of public		of .	specified in	
national	to them;		measure in	the	authorities		processing	principle 8. It	
legislations is	c) to be		a	fundamen	- person		to each	is desirable	
not justified.	given		democratic	tal rights	responsible's		recipient to	that the	
	reasons if		society in	and	legitimate		whom the	provisions of	
	i casons II		Journal of the state of the sta		iegitiiilate	1			

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 subparagr aphs (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 constitute s a necessary and proportio nate measure in a democrati c society for: - protection of national security, defence, public safety, important economic and financial interests of the State, the impartialit y and independe nce 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 disproporti onate 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 (humanitaria n clause)	
--	---	---	---	---	--	--	--	--

1		T T
purposes	judiciary	provided that
and where	or the	such
there is	preventio	departures
obviously	n,	are expressly
no risk of an	investigati	specified in a
infringemen	on and	law or
t of the	prosecutio	equivalent
privacy of	n of	regulation
the data	criminal	promulgated
subjects.	offences	in
	and the	accordance
	execution	with the
	of criminal	internal legal
	penalties,	system which
	and other	expressly
	essential	states their
	objectives	limits and
	of general	sets forth
	public	appropriate
	interest;	safeguards.
	and the	
	protection	
	of the	
	data	
	subject or	
	the rights	
	and	
	fundamen	
	tal	
	freedoms	
	of others,	
	notably	

freedom
of
expression
·   ·
Restriction
s 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
recognisa
ble risk of
infringem

		T T		1
	ent of the			
	rights and			
	fundamen			
	tal			
	freedoms			
	of data			
	subjects.			
Data		31. Right to	Article 18:	
subject		the	Right to	
rights:		Limitation of	restriction	
Dight to		treatment of	of	
Right to restriction		Personal	processing	
of		Data –	– The data	
		Holder shall	subject	
processing		have the	shall have	
		right to have	the right to	
		the	obtain from	
+		treatment of	the	
Exemptions		its personal	controller	
		data limited	restriction	
		to its storage	of	
		during the	processing	
		period of	where the	
		time	data subject	
		between a	contests its	
		rectification	accuracy,	
		or opposition	the	
		request, until	processing	
		its resolution	is unlawful,	
		by the	the	

person	controller
responsible.	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.
	0.11.1.40
	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	30.Right to	Article 20:	
subject	Portability of	Right to	
rights:	Personal	data	
Portability	Data –	portability	
1 of cability	Holder has	– The data	
	the right to	subject	
+	obtain a copy	shall have	
Exemptions	of personal	the right to	
Exemptions	data	receive	
	provided	their	
	(telephone or	personal	
	automated)	data which	
	in a structured	they have	
	electronic	provided to a controller,	
	format, that	in a	
	allows them	structured,	
	to use or	commonly	
	transfer to	used and	

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

		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	Article 9:	29. Right not	Article 22:	Article 35:
subject	Rights of	to be subject	Automated	Basis of a
rights:	the data	to	individual	Court decision
	subject –	Automated	decision-	– Art 35, 1: No

Automated		Every	Individual	making,	court decision
decisions		individual	Decisions –	including	implying an
		shall have	Holder shall	profiling –	assessment of
		a right not	have the	The data	the behaviour
+		to be	right not to	subject	of an
Exemptions		subject to	be the	shall have	individual
-		a decision	subject of	the right	shall be based
		significantl	decisions	not to be	on the
		y affecting	causing	subject to a	processing by
		him or her	significant/	decision	automatic
		based	legal effects,	based solely	means of
		solely on	based only	on	personal data
		an	on	automated	for the
		automate	automated	processing,	purpose of
		d	treatments	including	evaluating
		processing	assessing,	profiling,	certain
		of data	analysing or	which	aspects of
		without	predicting	produces	their
		having his	professional	legal or	personality.
		or her	performance,	other	Art 35, 2: no
		views	economic	similar	decision that
		taken into	situation,	effects,	has legal
		considerat	health status,	unless the	effect on an
		ion	sexual	decision is	individual
			preference,	necessary	shall be based
			reliability, or	for entering	solely on
		Exemptio	behaviour.	into, or	processing by
		n		performanc	automatic
		If the		e of, a	means of
		decision is	Exemption	contract	personal data
		authorised		between	for the
		authorised		the data	101 1110

by a law	- necessary	subject and	purpose of
to which		a data	defining the
the	execution of	controller;	profile of the
controll	er an	is	subject or
is subject	ct agreement	authorised	evaluating
and whi	_	by Union or	certain
also lay:	holder and	Member	aspects of
down	the person	State law to	their
suitable		which the	personality.
measur	20	controller is	' '
to	- holder	subject and	
safegua	rd consent	which also	
the data	Though in	lays down	
subject		suitable	
rights,	the holder	safeguards;	
freedon	ns has the right	or is based	
and	to obtain	on the data	
legitima	te human	subject's	
interest	s. intervention,	explicit	
	receive an	consent.	
	explanation,	The data	
Exception	on and appeal	controller	
s and	the decision.	shall	
restricti	on		
s:		implement suitable	
Article 1		safeguards, at least the	
Exception	on		
s and		right to obtain	
restricti		human	
s – whe	n		
such an		interventio	

	exception is provided for by law, respects the essence of the fundamen tal rights and freedoms and constitute s a necessary and proportio nate measure in a democrati c 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 impartialit	
and financial interests of the State, the impartialit	
financial interests of the State, the impartialit	
interests of the State, the impartialit	
of the State, the impartialit	
State, the impartialit	
impartialit	
y and	
independe	
nce of the	
judiciary	
or the	
preventio	
n,	
investigati	
on and	
prosecutio	
n 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	
subject of the rights	
the rights	
and	
fundamen	
tal	
freedoms	
of others,	
notably	
freedom	
of	
expression	
Restriction	
s may be	
provided	
for by law	
with	
respect to	
data	
processing	
for	
archiving	
purposes	
in the	
public	
interest,	
scientific	
or or	

			historical research purposes or statistical purposes where there is no recognisa ble risk of infringem ent of the rights and fundamen tal freedoms of data subjects.			
Accountab- ility standards						
Accountabi lity standards: Data protection officer	The appointment of one or more data protection or privacy officers, with		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	controllers	a personal	must	
qualifications,	and,	data	designate a	
resources and	where	protection	data	
powers for	applicable,	officer when:	protection	
exercising	processors	officer when.	officer in	
their	, take all	- it is a public	certain	
supervisory	appropriat	authority	cases, and	
functions			their	
	e	- purpose of		
adequately.	measures	treatment is	position	
The	to comply	the regular or	and tasks	
responsible	with the	systematic	are	
person and	obligation	observation	specified.	
any	s of this	of holder's		
processing	Conventio	conduct		
service	n and be	- performs		
provider must	able to	treatments		
protect the	demonstr	where a high		
personal data	ate, ()	risk to the		
subject to	that the	data		
processing	data	protection		
with the	processing	rights of		
appropriate	under	holders is		
technical,	their	likely		
organizational	control is	likely		
measures to	in	- if none of		
ensure each	complianc	the above		
time, their	e with the	apply, a data		
·	provisions	protection		
integrity,	of this	officer can		
confidentiality	Conventio	still be		
and	n.	appointed.		
availability.		11		

Dependent on	Explanato	
existing risk,	ry Report	
possible	Article 87:	
consequences	A possible	
to the data	measure	
subjects,	that could	
sensitivity of	be taken	
personal data,	by the	
the context of	controller	
processing	to	
and	facilitate	
obligations as	such a	
set out in	verificatio	
national	n and	
legislation.	demonstr	
	ation of	
	complianc	
	e would	
	be the	
	designatio	
	n of a	
	"data	
	protection	
	officer"	
	entrusted	
	with the	
	means	
	necessary	
	to fulfil his	
	or her	
	mandate.	
	Such a	

Accountabi	Data Subjects	15. A data	Member economies	data protection officer, whose desig- nation should be notified to the super- visory authority, could be internal or external to the controller.  Article	22. Notice of	Article 33	
lity standards: Breach prevention, response plans and reporting measures	should be informed by those involved in any stage of the processing of any security breach that could significantly affect their pecuniary or non-	controller should:  a) Have in place a privacy managem ent programm e that: i. gives effect to these Guidelines	should consider encouragin g controllers to develop and implement Privacy Manageme nt Programme s, which should provide	7.2: Each Party shall provide that the controller notifies, without delay, at least the competen t supervisor y authority	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,	Notification of a personal data breach to the supervisory authority – must be reported within 72 hours unless the breach is unlikely to	

	£		<u> </u>	/ \ - 5	:llasalas	T		Π
pecuniary	for all	appropriat		() of	illegal or		result in a	
rights, as well	personal	e safeguards,		those data	unauthorized		risk to the	
as measures	data	establish		breaches	alteration,		rights and	
taken for	under its	internal		which may	destruction		freedoms of	
resolution.	control;	oversight		seriously	or access,		data	
Information	ii. is	mechanism		interfere	unless the		subjects.	
should be	tailored to	s and		with the	violation		Article 34:	
provided in	the	responses		rights and	does not		Communica	
good time to	structure,	to		fundamen	pose a risk to		tion of a	
enable data	scale,	incidents.		tal	the holder's		personal	
subjects to	volume	Member		freedoms	rights and		data breach	
see	and	economies		of data	freedoms.		to the data	
protection of	sensitivity	should		subjects.			subject –	
their rights.	of its	consider					controller	
States should		encouragin					must	
	operations	g or					inform the	
encourage	′	requiring						
through their domestic law,	iii.	controllers					data subject if a breach	
•	provides	to provide						
implementati	for	notice to					is likely to	
on by those	appropriat	PEAs in the					result in a	
involved in	e	event of a					high risk to	
any stage of	safeguards	significant					their rights	
the	based on	security breach.					and	
processing of	privacy	breach.					freedoms.	
measures to	risk							
promote	assessmen							
better	t;							
compliance	',							
with	iv. is							
applicable	integrated							
laws on the	into its							

protection of	governanc
privacy with	e   e
regarding to	structure
the	and
processing of	establishe establishe
personal data	: s internal
The	oversight
implementati	mechanis
on of	ms;
procedures to	v. includes
prevent and	plans for
detect	
breaches,	respondin
which may be	g to inquiries
based on	inquiries and
standardized	incidents;
models of	incidents,
information	vi. is
security	updated in
governance	light of
and/or	ongoing
management.	monitorin
The	g and
implementati	periodic
on of a	assessmen
response plan	,   t;
that	b) Be
establishes	
guidelines for	to prepared
action in case	
of verifying a	
or verifying a	ate its

breach of	privacy
applicable	managem
laws on the	ent   ent
protection of	programm
privacy with	e as
regard to the	appropriat appropriat
processing of	e, in
personal data	, particular
including at	at the
least the	request of
obligation to	a
determine the	e competen
cause and	t privacy
extent of the	enforcem
breach, to	ent
describe its	authority
harmful	or another
effects and to	entity
take the	responsibl
appropriate	e for
measures to	promoting
avoid future	adherence
breaches.	to a code
	of conduct
	or similar
	arrangem
	ent giving ent giving
	binding
	effect to
	these

Guidelines
; and
c) Provide
notice, as
appropriat appropriat appropriat
e, to
privacy
enforcem
ent   ent
authoritie
s or other
relevant
authoritie
s 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
SIIUUU

Accountabi lity standards: Training	The periodic implementati on 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	notify affected data subjects.	Explanato ry Report Article 85: According to article 10 paragraph 1, the obligation on the controller to ensure adequate data protection is linked to the responsibi	20. Responsibilit y principle – training noted as a mechanism to adopt to comply with this principle.	Article 24: Responsibili ty of the controller  The controller shall implement appropriate technical and organisatio nal measures to ensure and to be able to demonstrat	
	protection of		the		and to be able to	

for that	complianc	measures
purpose.	e with the	shall be
	applicable	reviewed
	law. The	and
	data	updated
	protection	where
	principles	necessary.
	set out in	Where
	the	proportiona
	Conventio	te in
	n, which	relation to
	are to be	processing
	applied at	activities,
	all stages	the
	of	measures
	processing	referred to
	, including	shall
	the design	include the
	phase, aim	implementa
	at	tion of
	protecting	appropriate
	data	data
	subjects	protection
	and are	policies by
	also a	the
	mechanis	controller.
	m for	
	enhancing	
	their trust.	
	Appropria	
	te	
	measures	

that the
controller
and
processor
may have
to take to
ensure
complianc
e include:
training
emp-
loyees;
setting up
appropriat appropriat
e   e
notificatio
n   n
procedure
s (for
instance
to indicate
when data
have to be
deleted
from the
system);
establishin
g specific
contractua
provisions
where the

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

applicable	to ensure	audits, noted	organisatio	
laws on the	adequate	as a	nal	
protection of	data	mechanism	measures	
privacy with	protection	to adopt to	to ensure	
regard to the	is linked to	comply with	and to be	
processing of	the	this principle.	able to	
personal data,	responsibi		demonstrat	
as well as	lity to		e that	
with the	verify and		processing	
procedures	be in a		is	
established by	position to		performed	
the	demonstr		in	
organization	ate that		accordance	
for that	data		with this	
purpose.	processing		Regulation.	
	is in		Those	
	complianc		measures	
	e with the		shall be	
	applicable		reviewed	
	law. The		and	
	data		updated	
	protection		where	
	principles		necessary.	
	set out in		Where	
	the		proportiona	
	Conventio		te in	
	n, which		relation to	
	are to be		processing	
	applied at		activities,	
	all stages		the	
	of		measures	
	processing		referred to	

Г	T T			
		, including	shall	
		the design	include the	
		phase, aim	implementa	
		at	tion of	
		protecting	appropriate	
		data	data	
		subjects	protection	
		and are	policies by	
		also a	the	
		mechanis	controller.	
		m for		
		enhancing		
		their trust.		
		Appropria		
		te		
		measures		
		that the		
		controller		
		and		
		processor		
		may have		
		to take to		
		ensure		
		complianc		
		e include:		
		training		
		employee		
		s; setting		
		up		
		approp-		
		riate		
		notific-		

T
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-

Accountabi	The	Promotion	ation and demonstration of compliance.	38. Privacy	Article 25:	
lity	adaptation of	of technical	Additional	Due to	Data	
standards:	information	measures	oblig-	Design and	protection	
	systems	to protect	ations –	Privacy by	by design	
Privacy by	and/or	privacy.	Each Party	<b>Default</b> – The	and by	
design	technologies	Member	shall	person	default –	
	for the	economies should	provide	responsible	Taking into	
	processing of	promote	that	shall apply	account the	
	personal data	technical	controllers	preventive	state of the	
	to the	measures	and,	measures	art, the cost	
	applicable	which help	where	from the	of	
	laws on the	to protect	applicable,	design stage.	implementa	
	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	privacy. Member economies may encourage controllers to make full use of readily available technical safeguards and measures, and may also	processors () shall design the data processing in such a manner as to prevent or minimise the risk of interf- erence with those	The person responsible shall guarantee that its programs, services, computing systems, applications or other technology that treats personal	tion and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of	

	implementati on thereof.	support the developme nt 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.	natura person posed the proces the contro shall, be at the soft the determation of means proces and at time of proces itself, implent appropriate the appropriate the solution of the design implent data	sing, ller oth cime nin- f the for sing the the sing anent oriate cal sat- res, sonym n, are ed to	
--	-----------------------------	--	----------------------------------	--	---	--	--

protection
principles,
such as data
minimisatio
n, in an
effective
manner and
to integrate
the
necessary
safeguards
into the
processing
in order to
meet the
requiremen
ts of this
Regulation
and protect
the rights of
data
subjects.
The
controller
shall
implement
appropriate
technical
and
organisatio
nal

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 storage and their accessibility		
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 screens and their accessibility		
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 storage and their accessibility		
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		
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		default,
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		only
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		personal
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 storage and their accessibility		data which
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 ftheir storage and their accessibility		are
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 ftheir storage and their accessibility		necessary
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		for each
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		specific
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		
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		
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		processing
That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility		
That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility		processed.
applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility		
applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility		obligation
the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility		
of personal data collected, the extent of their processing, the period of their storage and their accessibility		
data collected, the extent of their processing, the period of their storage and their accessibility		of personal
the extent of their processing, the period of their storage and their accessibility		
the extent of their processing, the period of their storage and their accessibility		collected,
processing, the period of their storage and their accessibility		
the period of their storage and their accessibility		of their
the period of their storage and their accessibility		processing,
of their storage and their accessibility		
storage and their accessibility		
their accessibility		
accessibility		
		. In

					particular not making personal data by default accessible to an indefinite number of persons.  An approved certification mechanism could assist in demonstrati ng the above.	
Accountabi	The		Article 10:	41. Impact	Section 3:	
lity	implementati		Additional	Assessment	Data	
standards:	on of privacy		<b>obligation</b> – Each	on the Protection of	protection	
Impact	impact assessments		party shall	Personal	impact assessment	
assessment	prior to		party snan	<b>Data</b> – The	and prior	
s	implementing		that	person	consultatio	
	new		controllers	responsible	n	
	information		and,	shall perform		
	systems		where	an impact	Article 35:	
	and/or		applicable,	assessment	Data	
	technologies		processors	prior to	protection	

for the	, examine	implementati	impact	
processing of	the likely	on of	assessment	
personal data,	impact of	treatment of	<ul><li>Where a</li></ul>	
as well as	intended	personal data	type of	
prior to	data	that probably	processing	
carrying out	processing	entails a data	in particular	
any new	on the	protection	using new	
method of	rights and	high risk.	technologie	
processing	fundamen	National	s, and	
personal data	tal	legislation	taking into	
or substantial	freedoms	shall set out	account the	
modifications	of data	the	nature,	
in existing	subjects	treatments	scope,	
processing.	prior to	that will	context and	
	the	require an	purposes of	
	commenc	impact	the	
	ement of	assessment;	processing,	
	such	its contents;	is likely to	
	processing	and the	result in a	
		requirements	high risk to	
		around	the rights	
		submission	and	
		to the control	freedoms of	
		authority.	natural	
			persons,	
			the	
			controller	
			shall, prior	
			to the	
			processing,	
			carry out an	
			assessment	

T			
		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	
	<u> </u>	P. 2 2 2 2 2 1 1 1 2	

					1	would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	
Accountability standards: Codes of conduct/practice; certification 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	ry Re Artic 127: addit to the constant of the coul whee other mea	tion ethics a certific system other seen system developed validate rules dalso established in nation to the perior of the period	tion inisms is of and ration is (and is) can ped, ed by shed onal cion. rson sible arily		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-	g personal	those	ions and	
compliance.	data	schemes,	other	
The	processing	whose	bodies,	
The	are in	purpose is	intended to	
responsible	prepar-	the correct	contribute	
person and	ation,	application of	to the	
those	such as for	the law, to	proper	
involved in	instance	establish	application	
processing	codes of	conflict	of this	
shall maintain	conduct or	resolution	Regulation,	
confidentiality	technical	between the	taking	
of personal	norms.	person	account of	
data. This		responsible	the specific	
obligation		and the	features of	
shall remain		holder.	the various	
even after the			processing	
ending of the			sectors and	
relationship			the specific	
with the data			needs of	
subject, or			micro, small	
with			and	
responsible			medium-	
person.			sized	
			enterprise.	
			Article 41	
			Monitoring	
			of	
			approved	
			codes of	
			conduct –	
			Codes will	

monitored by a body accredited by the competent supervisory authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		I. I. I	
by a body accredited by the competent supervisory authority.  Article 42: Certific- ation — Member States, the supervisory authoritles, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		be	
accredited by the competent supervisory authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for			
by the competent supervisory authority.  Article 42: Certification — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for			
competent supervisory authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for			
supervisory authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		by the	
authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		competent	
authority.  Article 42: Certific- ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		supervisory	
Certification — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		authority.	
ation — Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		Article 42:	
Member States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for			
States, the supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		ation –	
supervisory authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for			
authorities, the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		States, the	
the Board and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		supervisory	
and the Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		authorities,	
Commission shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		the Board	
shall encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		and the	
encourage the establishme nt of data protection certification mechanism and of data protection seals and marks, for		Commission	
the establishme nt of data protection certification mechanism and of data protection seals and marks, for		shall	
establishme nt of data protection certification mechanism and of data protection seals and marks, for		encourage	
nt of data protection certification mechanism and of data protection seals and marks, for		the	
protection certification mechanism and of data protection seals and marks, for		establishme	
protection certification mechanism and of data protection seals and marks, for		nt of data	
certification mechanism and of data protection seals and marks, for			
mechanism and of data protection seals and marks, for			
and of data protection seals and marks, for			
protection seals and marks, for			
seals and marks, for			
marks, for			
		the purpose	

						of demonstrati ng compliance.  Article 43: Certificatio n bodies – Certification bodies will be accredited.	
Accountability standards: Records of processing activities	Implied by accountability requirements.	Implied by accountab ility requireme nts.		Implied by accountab ility requireme nts.	Implied by accountability requirements.	Article 30: Records of processing activities – Each controller and, where applicable, the controller's representat ive, shall maintain a record of processing activities under its responsib- ility. Article 30 lists	

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

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.  The same shall apply to personal data relating to criminal convictions  The same shall apply to personal data relating to criminal convictions  The same shall apply to personal data relating to criminal convictions  The same shall apply to personal data relating to profibitical relating to criminal convictions  The same shall apply to personal data applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  The same shall apply to personal data applicable by national legislation on with due guarantees of any additional conditions established to preserve the rights of the data subject.  The same shall apply to personal data apply sain applicable by national legislation on with due guarantees of any additional conditions established to preserve the rights of the data subject or appropriat e enshrined in law complements are enshrined in law complements of the data subject or another appropriat e enshrined in law complements of the data subject or another appropriat enshrined in law complements of the data subject or another appropriat enshrined in law complements are enshrined in law complements are appropriate to the data subject or another appropriate enshrined in law complements apply such a natural and enshible to person, data autival concerning the data subject or data subject or an antural person's sex life or sexual enshible or protect the vital interests of the data subject or another appropriate enshrined in law complements appropriate to the data subject or another appropriate enshrined in law complements appropriate enshrined in law complements and obligations in trule state their actions.  The same stricted 30 — data subject or data subject or another subject until the profit of the data subject or	philosophical	safeguards.	relating to	treated	health data,	uniquely	membership	exceptions to
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.  **Note of any additional conditions established to preserve the rights of the data subjects.**  **All apply to personal data may additional conditions established to preserve the rights of the data subjects.**  **All apply to personal data make public opinions, tradeunion membersh lip, religious or other beliefs, health or sexual life, with a legal allowed where appropriat enshrined in law complementing those of this Convention.**  **All apply to personal data subject opinions, tradeunion membersh lip, religious or other beliefs, health or sexual life or sexual or or another person apply and the problem of the data subject the vital interests of the data subject or another person apply such a personal person, data subject compliance with powers and subject or onsents and relation shift of the data subject the vital interests of the data subject or another person apply and the person apply to the data subject or obligations in religious or other beliefs, health or sexual life, with a legal matural person, data on the public compliance with powers and subject or onsents and relation shift of the data subject the vital interests of the data subject or on another person apply, such and the problem of a number of a	l ·	_			,		·	•
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.  At a subjects.  To personal data political political relating to criminal convictions or other beliefs, health or sexual life, shall only be allowed where appropriate enshrined in law complements and safeguards are enshrined in law complements and the public or preserve the rights of the data subjects.  To personal data political political relating to convictions or other beliefs, health or sexual life, shall only be allowed where appropriate enshrined in law complements and the public security, public order, public security, public order, public health, or the safekeeping of the rights of the gata and and and the public security or processary for necessary for preceived in the public security or the safekeeping of the rights and the public security or the safekeeping of the rights and the public security or the safekeeping of the rights and the public security or the sec						, ,		
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.    Ada	·	1		•				•
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.  I data subjects.  I relating to criminal convictions applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  I data subject with powers and membersh ip, religious or other beliefs, health or sexual life, with a legal mandate of allowed where appropriate e appropriate in law complementing those of this Conventio n.  I data subject with data subject and manifestly made public or concerning a natural consent or life or sexual or concerning a natural consent or legal claims singlect or of a number of sexual or elementary or sexual or concerning a natural consent or legal claims singlect or of a number of sexual or concerning an antural consent or legal claims subject or of a number of sexual or concerning health or concerning an antural consent or legal claims or legal claims are upor print in law complementary or sexual from the public or consents and manifestly made public or onsents or legal claims and antural very consent or legal claims or interests of the data subject or consents of the data subject or consent or legal claims are upor print in law complementary or sexual from the public or consent or legal claims or interest of the data subject or consents and and are processary to protect the vital interests of the data subject or consents and or interest of the data subject or consents and or interest or sexual or consent or the vital interests of the data subject or consents another or processing necessary to protect the vital interests of the data subject or consents and or interest, in the public or on the provided that an antural very processing necessary to protect the vital interests of the data subject or consent and the provided that an antural very processing necessary to protect the vital interests of the data subject or consent and the provided		•	_	-	,	•		
may apply as applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  In a convictions and convictions applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  In a convictions applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  In a convictions and convictions and membersh ip, religious or other beliefs, health or sexual life, shall only be allowed where appropriat enshrined in law comsents are enshrined in law compliance with powers and obligations in rules that regulate their actions shall be vital interests of the data subject onsents and onsent regulate their actions with a legal mandate of the data subject onsents are enshrined in law consent, niting those of this conventio n.  In a convictions and whore subject on the protect the vital interests of the data subject onsent or protect vital interests of another of a natural consent regulate their actions sexual onsent or protect vital interests of the data subject onsents accurity, public order, public order, public entered in the public order, public order, public entered in the public onsent, and the public order of the fights and order or protect vital interests of an antural consent regulate their actions with a legal mandate of the data subject onsent regulate their actions and recessary to protect the vital interests of the data subject onsent regulate their actions sexual or onsent, and onsent regulate their actions another of a natural consent regulate their actions another protect vital interests of the data subject vital interests o			-	•	•		· · · · · · · · · · · · · · · · · · ·	
applicable by national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  A subjects.  Convertions  union membersh ip, religious or other bellefs, health or sexual life, shall only be allowed where appropriat e enshrined in law complementing those of this Conventio n.  A subject on data subject consent of the data subject or another person sexual subject on processing to protect the vital interests of the data subject or another person sexual oconsent of the vital interests of the data subject or another person sexual oconsent of the vital interests of the data subject or another person conditions genetic data) and any of the rights of the data subject or another person sexual oconsent of the vital interests of the data subject or another person conditions genetic data) and proceedings or criminal investing ations of the rights and on the public occurrity or interest, in the public occurring anatural concerning anatural concerning anatural regulate their actions or orientation occurring anatural regulate their actions or required to protect the vital interests of the data subject or sexual fregulate their actions or processing and antural regulate their actions or required to protect the vital interests of the data subject or another person sexual file or protect the vital interests of the data subject or another regulated for prospects with a legal unless one of a number of		_		•	= = = = = = = = = = = = = = = = = = =	_		
national legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.  In a subjects.  In a subject ip, religious or other beliefs, health or established to preserve the rights of the data subjects.  In a subject ip, religious or other beliefs, health or established to preserve the rights of the data subjects.  In a subject in the data subject ip, religious or other beliefs, health or established to preserve the rights of the data subjects.  In a subject in the data subject in the person's sex life or encessary to protect the wital interests of the data subject or enother of the data subject or enotest inferencessary to protect the wital interests of the data subject or enother or enother of the data subject or enotesting in the public order, public order, public order, public health, or the safekeeping of the rights of the data subject or enotesting an autural consent of the data subject or entered on entered in the prohibited or entered or enother of the data subject on entered in the prohibited or entered in the prohibit				•	subject		complica.	•
legislation with due guarantees of any additional conditions established to preserve the rights of the data subjects.    Possible of preserve the rights of the data subjects.   Possible of preserve the rights of the data subjects.   Possible of preserve the rights of the data subjects.   Possible of preserve the rights of the data subjects.   Possible of preserve the rights of the data subjects.   Possible of protect the vital interests of the data subject or another person   Possible of the data subject   Possible of the data subject   Possible or another person   Pos					- data subject			•
with due guarantees of any additional conditions established to preserve the rights of the data subjects.  In the data subjects.  In the data subjects.  In the data subject shar regulate their actions or other beliefs, health or preserve the rights of the data subjects.  In the data subjects.  In the data subject shar regulate their actions or other beliefs, health or preserve the rights of the data subjects.  In the data subjects.  In the data subject shar regulate their actions or they comply sexual life or sexual orientation shall be prohibited unless one subject the vital interests of the data subject or another of anumber of an number of person's sex life or sexual orientation shall be prohibited unless one subject the vital interests of the data subject or another of an number of a				_	_	•		•
guarantees of any additional conditions established to preserve the rights of the data subjects.    Security, public order, ormplementing those of this Conventio n.					_			subject
any additional conditions established to preserve the rights of the data subjects.    Sexual life, shall only be allowed where appropriat e enshrined in law complementing those of this Convention in.   Sexual life, shall only be allowed where appropriat this convention in.   Sexual life, shall only with a legal mandate of the data subject or sexually orientation shall be prohibited orientation shall be prohibited orientation shall be prohibited unless one of the data subject or another of a number of a nu			_	_	Consent	•		- written
conditions established to preserve the rights of the data subjects.  health or sexual life, shall only be allowed where appropriat e months are enshrined in law compleme nting those of this Conventio n.  health or sexual life, shall only be shall only be allowed where appropriat e months are enshrined in law complements this Conventio n.  health or sexual life, with a legal mandate of the data subject the vital interests of the data subject or another consents allowed unless one of a number of the data subject or another person conditions apply, such as explicit consent, public order, public order, public health, or the consents and rights in employmen to for reasons of the rights and rone employmen to for reasons of the public security or the protect the vital interests or protect the vital interests of the data subject or another prohibited unless one of a number of conditions apply, such as explicit consent, necessary for as explicit consent, or procedures, or				actions		sexual		
established to preserve the rights of the data subjects.    Sexual life, shall only be allowed where appropriat e enshrined in law compleme nting those of this Conventio n.	·			- they comply	-			
preserve the rights of the data subjects.    Shall only be allowed where appropriat e enshrined in law complementing those of this Conventio n.	established to		sexual life,		•	shall be		,
rights of the data subjects.  be allowed where appropriat e appropriat e enshrined in law compleme those of this Conventio n.  compleme those of this conventio and not convention n.  convention of the data subject or another consents subject or another of a number of a number of a number of anumber of anumber of anumber of conditions apply, such as explicit consent, necessary for as explicit consent, necessary for as explicit consent, necessary for public order, public health, or the safekeeping of the rights and rights in employmen to the public security or secur	preserve the		shall only	_		prohibited		•
where appropriat e appropriat e safeguards are enshrined in law compleme nting those of this Conventio n.  allowed where appropriat e appropriate e	rights of the		be			unless one		•
where appropriat e appropriat e safeguards are enshrined in law compleme those of this Conventio n.  where appropriat e appropriat e appropriat e appropriat e appropriat safeguards are enshrined in law compleme those of this conventio n.  where appropriat e appropriational appropriation approp	data subjects.		allowed		•	of a number		interests
appropriat e for national safeguards are enshrined in law compleme those of those of those of Conventio n.  appropriat e for national safeguards security, public order, public health, nting of the rights and  appropriat - necessary for national security, public security, public order, public health, or the safekeeping of the rights and - necessary in those of the rights and - necessary toredicata) apply, such as explicit legal claims or consent, necessary - judicial procedures, criminal investing- ations - necessary obligations or criminal investing- ations - necessary for proceedings or criminal investing- ations - necessary for procedures, criminal investing- ations - necessary in the public security or interest, in			where	consents		of		- (in particular
e safeguards are public security, public order, compleme those of this Conventio n.  e safekeeping of the rights  n.  e safeguards security, public order, public of the rights  are public security, public order, public health, or the safekeeping of the rights  n.  e for national security, public required for legal claims security, necessary for legal claims on the security, public order, public health, or the safekeeping of the rights  and - processing required for legal claims on the security, necessary for legal rights  necessary for obligations or criminal investing- ations  and rights in - necessary for as explicit consent, necessary for security or consent, necessary for as explicit consent, necessary for obligations and rights in and rights in a security or security or security or security.			appropriat	- necessary	person	conditions		
are enshrined in law compleme those of this Conventio n.  are enshrined in law enshrined in law compleme those of this conventio n.  are enshrined enshrined in law security, public order, public health, or the safekeeping of the rights and rights  security, public order, public health, or the safekeeping of the rights and rights  - judicial procedures, criminal investigations in employmen for reasons of the public security or interest, in			е	•	- processing	apply, such		•
enshrined in law compleme nting those of this Conventio n.  enshrined in law security, public order, public health, or the safekeeping of the rights  Conventio n.  enshrined security, public order, public health, or the safekeeping of the rights  and rights  in ecessary for obligations or criminal investigations  in employmen t, social security or interest, in			safeguards	security,	required for	as explicit		legal rights
in law compleme nting those of this Conventio n.    In law compleme nting those of the rights of this conventio n.    In law compleme nting those of the rights of the rights of the rights of the rights of the public the public the lath, or the safekeeping of the rights of the rights of the rights of the public the public the lath, or the public the public the lath, or the public the lath			are	public	legal claims	consent,		
compleme nting those of this Conventio n.  That compleme nting those of the rights and nting this conventio n.  That compleme nting compleme nting those of the rights and nting those of the rights and nting the public to receive the procedures, or initial to obligations and rights in the public to receive the procedures, or initial to the public to receive the procedures, or initial to receive the procedures, or initial to receive the procedures, or initial to the public to receive the procedures, or initial to receive the procedures, or initial to receive the procedures, or initial to the public to receive the procedures, or initial to receive the procedures, or initial to receive the procedures, or initial to receive the procedures the procedure the procedures the procedure the pro			enshrined	security,		necessary		_
nting those of this Conventio n.  Conventio n.  Complete public health, or the safekeeping of the rights and rights in employmen the public health, or the safekeeping ations  In criminal investigations and rights in employmen the public health, or the safekeeping ations  In criminal investigations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the public health, or the safekeeping ations and rights in employmen the safekeeping ations and rights in employmen the safekeeping ations at the public health, or the safekeeping ations and rights in employmen the safekeeping ations at the public health, or the safekeeping ations and rights in employmen the safekeeping ations and safekeeping at the safekee			in law	public order,	_			
those of this conventio n.  Titing those of those of those of this safekeeping of the rights and this convention n.  Titing to refer the safekeeping of the rights alions to the public				public health,	•	_		
this conventio n. safekeeping of the rights and safekeeping of the rights ations safekeeping of the rights and safekeeping of the rights ations safekeeping of the rights at the rights			_	or the		_		investigations
this Conventio n. of the rights and of the rights and the public t				safekeeping				- necessary
n. The cessary in the public security or interest, in				of the rights	ations	• •		-
the public ' little est, in			Conventio	and	- necessary in	*		public
interest Social narticular for			n.		the public	•		interest, in
particular for					interest,	social		particular for

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

, religious,	purposes, for p	oolitical,
cooperative		osophical,
or trade		ious,
union aim	archiving in mut	
anion ann		efit or
- literary or		e union
artistic	· ·	oses.
expression/	scientific	,0363.
journalism,	research	
National law	purposes.	
with regard	pa.poses.	
to print		
media or the		
audio-visual		
sector still		
applies.		
No decisions		
producing		
legal or othe	r	
significant		
effects based	I	
solely on		
automated		
processing.		
No transfers		
to non-		
Member		
States unless		
an adequate		
level of		
protection is		

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

	<u> </u>	T		
this	s. The	which		
Resolution	instruction	establishes		
and	s given by	subject,		
applicable	the	scope,		
national	controller	contents,		
legislation;	establish	duration,		
and	the limit	nature and		
b. the legal	of what the	purpose,		
relationship	processor	type of personal		
established	is allowed	data. Certain		
through a	to do with	general		
contract or	the	clauses must		
legal	personal	be included		
instrument	data.	in the		
that allows		agreement.		
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				

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

processing	respective
processing	responsibilit
<i>\frac{1}{2}</i>	
	ies 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
	arrangemen
	t between
	them
	unless, and
	in so far as,
	the
	respective

			responsibilit ies 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.
			subjects.
Specific themes/ requiremen ts:  Vulnerable or other groups of data subjects, e.g. children	Article 15: Supervisor  y authoritie s - authoritie s 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 responsibi lities under this Conventio n - 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 responsibilit y over the child.  Article 12: Transparen t information - Information relating to processing should be communica ted in a concise, transparent , intelligible and easily accessible		T			
parental responsibilit y over the child.  Article 12: Transparen t information — Information relating to processing should be communica ted in a concise, transparent , intelligible and easily			individuals		
responsibilit y over the child.  Article 12: Transparen t information — Information relating to processing should be communica ted in a concise, transparent , intelligible and easily				holder of	
y over the child.  Article 12: Transparen t information — Information relating to processing should be communica ted in a concise, transparent , intelligible and easily				parental	
y over the child.  Article 12: Transparen t information — Information relating to processing should be communica ted in a concise, transparent , intelligible and easily				responsibilit	
child.  Article 12: Transparen t information  Information relating to processing should be communica ted in a concise, transparent , intelligible and easily					
Article 12: Transparen t information — Information relating to processing should be communica ted in a concise, transparent , intelligible and easily					
Transparen t information  - Information relating to processing should be communica ted in a concise, transparent , intelligible and easily					
t information  Information  relating to processing should be communica ted in a concise, transparent , intelligible and easily					
information  Information  Information  relating to processing should be communica ted in a concise, transparent , intelligible and easily					
Information relating to processing should be communica ted in a concise, transparent , intelligible and easily					
Information relating to processing should be communica ted in a concise, transparent , intelligible and easily				information	
relating to processing should be communica ted in a concise, transparent , intelligible and easily					
processing should be communica ted in a concise, transparent , intelligible and easily					
should be communica ted in a concise, transparent , intelligible and easily					
communica ted in a concise, transparent , intelligible and easily					
ted in a concise, transparent , intelligible and easily				should be	
concise, transparent , intelligible and easily				communica	
transparent , intelligible and easily				ted in a	
, intelligible and easily				concise,	
and easily				transparent	
				, intelligible	
accessible				and easily	
				accessible	
form, using				form, using	
clear and					
plain					
language, in					
particular					
for any					
information					
				addressed	

				specifically	
				to a child.	
Specific				Article 90	
themes/				Obligations	
requiremen				of secrecy –	
ts:				Member	
				States may	
professiona				adopt	
I secrecy				specific	
and				rules to set	
supervisory				out the	
authority				investigativ	
investigatio				e powers of	
ns				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	

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

							or has obtained in an activity covered by that obligation of secrecy.		
Compliance	Monitoring	The API		Article 15:	42. Nature of	Article 11:	Article 51:	Supervision	Article 14:
and	In every State,	Framew	1.01000.10	Supervisor	Control and	Status,	Supervisory	and	Establishment
monitoring	there shall be	can be enforce	the	У	Supervision	composition	authority –	sanctions –	– within the
:	one or more	via vario	Convention	authoritie	Authorities –	and	Each	The law of	ECOWAS
Independe	supervisory	models	as for the	s – Each	There must	organization	Member	every	space, each
nt	authorities, in	deemed	Protection	Party shall	be one or	of National	State shall	country shall	Member State
supervisory	accordance	approp	1 - 1 - 1 - 1 -	provide for one or	more control authorities	Personal Data	provide for	designate the authority	shall establish its own data
authorities'	with domestic	e by the		more		Protection	one or more	which, in	protection
powers and	law, that will	membe		authoritie	on personal data	Authorities –	independen	accordance	Authority. It
competenc	be	econom questio	<b>y</b>	s to be	protection in	Each State	t public	with its	shall be an
es	responsible	Can inc		responsibl	each Ibero-	Party shall	authorities	domestic	independent
	for	Privacy	of Personal	e for	American	establish an	to be	legal system,	administrative
	supervising	Enforce		ensuring	State.	authority in	responsible	is to be	Authority
	the	nt	regarding	complianc	Control	charge of	for	responsible	responsible
	observance of	Authori	supervisory	e with the	authorities	protecting	monitoring	for	for ensuring
	the principles	(PEAs),	authorities	provisions	shall be free	personal	the	supervising	that personal
	set out in the	multi-	and	of this	of any	data. It shall	application	observance	data is
	Resolution,	agency enforce	me transborder	Conventio	external	be an	of this	of the	processed in
	who shall be	nt bodie	1	n. Article	influence and	independent	Regulation.	principles.	compliance
	impartial and	networ	, I	contains	shall not	administrativ	Article 55	This	with the
	independent, and will have	of		detailed	request nor	e authority		authority	provisions of
	and will have	designa	ted	requireme	admit any	with the task	Competenc	shall offer	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	industry bodies, courts and tribunals, or a combinatio n of the above.  However, member economies are encourage d to establish PEAs, and those that are established should be provided with the governance , resources and technical expertise	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	nts, including powers of investigati on and interventi on; approval of safeguards for transbord er data flows; powers to issue decisions and impose administra tive sanctions, and to engage in legal	order or instruction.  Applicable national legislation must grant control authorities sufficient investigation, resolution, promotion, sanction and other powers necessary to guarantee effective compliance.  Control authorities must have the necessary human and	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	e – Each supervisory authority shall be competent for the performanc e 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	guarantees of impartiality, independenc e 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 implementin g the aforementio ned	Supplementar y Act.  Article 19: Responsibiliti es – 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
applicable national legislation on the protection of privacy	should be provided with the governance , resources and	effect to the principles stated in Chapters II and III of	impose administra tive sanctions, and to	effective compliance.  Control authorities must have	for opinions, informing persons concerned and data controllers of	on the territory of its own Member State.	provisions of the national law implementin g the aforementio	processing, dealing with claims, petitions and complaints, judicial

remedy before the supervisory authorities referred to, including judicial oversight of	participate in the APEC Cross- border Privacy Enforceme nt Arrangeme nt (CPEA)	in particular, powers of investigatio n and interventio n, as well as the power	proposals for any legislative or administra tive measures which	notifications of processing, dealing with claims, petitions, complaints, judicial	monitoring and	the appropriate individual remedies.	of personal data processing, authorizing transborder transfers, establishing cooperation
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.	one Privacy Enforceme nt Authority. Defines 'Privacy Enforceme nt Authority' as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigatio ns or pursue enforceme	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.	for the processing of personal data.  Each Party shall ensure that the supervisor y authoritie s are provided with the resources necessary for the effective performan ce of their functions	offences, audits, imposing administratice and monetary sanctions, authorizing transborder transfers, establishing cooperation mechanisms. Authorities may also issue official warnings, followed by withdrawal of authorizations and	include investigatio n, corrective powers, authorisatio n and advisory powers.		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 fundamenta I freedoms with regard to the processing of personal data within its competenc e.	and exercise of their powers.  Authoritie s shall not be competen t 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 independe nce of	Supervisory authorities shall be impartial and independent, and will have technical competence, sufficient	Cross- border Privacy Enforcement Arrangem nt defines 'Privacy Enforcement	for the Protection of Individuals	Article 15: Superv- isory authoritie s - supervisor y authoritie s 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: Independen ce  1. Each supervisory authority shall act with complete	The authority shall offer guarantees of impartiality, and independenc e vis-à-vis persons or	Article 16: Incompatibility – membership of the data protection Authority shall be incompatible

supervisory	powers and	Authority'	to	with	influence and	Authorities –	independen	agencies	with
authorities	adequate	as any	Automatic	complete	shall not	Each State	ce.	responsible	membership
	resources to	public body	Processing	independ-	request nor	Party shall		for	of
	deal with	that is	of Personal	ence and	admit any	determine	2. The	processing	government,
	claims by data	responsible	Data	impartial-	order or	the	member or	and	the exercise of
	subjects.	for	regarding	ity in	instruction.	composition	members of	establishing	business
		enforcing	supervisory	perform-		of the	each	data.	executives,
		Privacy Law, and	authorities	ing their	Members	national	supervisory		and
		that has	and	duties and	shall be	personal data	authority		ownership
		powers to	transborder	exercising	appointed	protection	shall remain		and shares in
		conduct	data flows:	their	through a	authority,	free from		businesses in
		investigatio		powers	transparent	but	direct and		the
		ns or	Article 1 –	and in	procedure	membership	indirect		information
		pursue	The	doing so	under	of the	external		and
		enforceme	supervisory authorities	shall	applicable	authority	influence, and shall		telecommunic
		nt proceeding	shall	neither	national	shall be	neither		ations sectors.
		s	exercise	seek nor	legislation and may only	incompatible	seek nor		Article 17:
		3	their	accept	be removed	with	take		Immunity –
			functions in	instruct-	due to	membership	instructions		members shall
			complete	ions.	serious	of	from		enjoy full
			independen		causes,	Government,	anybody.		immunity in
			ce.		established	business	anybody.		respect of
			cc.		in the	executive	3. Member		opinions
					internal law	and	or members		expressed in
					or each	ownership of	of each		the exercise
					State,	shares in the	supervisory		of, or during
					according to	information	authority		the tenure of
					the rules of	and	shall refrain		their function.
					due process.	communicati	from any		They shall
						on	action		receive no
					Decisions of		incompatibl		instructions
					the control		e with their		

						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 e 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 infrastructure		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
	WITICIT STIGIT

	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
	independen
	ce and that
	it has
	separate,
	public
	annual
	budgets,

Compliance	The	Member	Article 13:	Article 17:	45.	which made be part of the overage state or national budget.  Article	:	
and	competent	economies	Cooperatio	Forms of	Establishmen	57(g): Tas	ks	
monitoring	supervisory	are encour-	n between	cooperati	t of	-		
:	authorities in	aged to	Parties –	on – The	International	Superviso	ry	
Cooperation	each State	share	the Parties	supervis-	Cooperation	authoritie	es	
Cooperatio	will make	informat- ion re	agree to	ory	Mechanisms	shall		
n with	every effort	matters	render each	authorit-	– Ibero-	cooperat	9	
other authorities	to share	that have a	other	ies shall	American	with,		
within the	reports,	significant	mutual	cooperate	States may	including		
framework	investigation	impact on	assistance	with one	adopt	sharing		
Halliework	techniques,	privacy	in order to	another to	international	informati	on	
	communicatio	protection,	implement	the extent	cooperation	and		
	n and	educate	this	necessary	mechanisms,	providing		
	regulatory	one	Convention.	for the	which may	mutual		
	strategies and	another,	Additional	performan	include:	assistanc	غ ا	
	any other	share investing-	Protocol to	ce of their	- mechanisms	to other		
	useful	ation	the	duties and	that allow	superviso	ry	
	information	techniques	Convention	exercise of		authoritie	es	
	for exercising	and	for the	their	reinforcing international	with a vie	w	
	their	regulatory	Protection	powers:	assistance	to ensuri	ng	
	functions	strategies.	of	including	assistance	the		
	more	APEC	Individuals	exchangin	cooperation	consister	су	
	effectively, in	Cross-		g relevant	in the	of		
	particular	border	with regard to	and useful	application of	application	n	
	when	Privacy	Automatic	informatio	application of	and		
		,	Automatic					

following a request for cooperation by another supervisory authority in conducting an investigation or intervention.  Conduct coordinated investigations	Enforceme nt Arrangeme nt (CPEA) facilitates sharing and provides mechanism s to promote effective cross- border enforceme nt  Process of Pers Data regardi supervi authori and transbo data flo	cooperate with each other, isory coordinati ing investigati ons or interventi ons, conductin g joint actions:	relevant national law assistance between control authorities through notification and submission of claims, assistance in investigation	enforcemen t of the Regulation.  Further detail is set out in Articles 56: Competenc e of the lead supervisory authority; 60:
the interests of two or more authorities are shared.  Take part in associations, working groups, joint fora, as well as seminars, workshops or	signed up to the arrangeme nt. An economy must participate in the APEC Cross- border Privacy Enforceme nt Arrangeme provision of Artic of the Conven the supervi authori shall co operate with or anothe the ext	cle 13 tive practice.  Authoritie s shall form a network in order to organise their cooperati	aimed at awareness and exchange of best practices.	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 Enforceme nt Authority.	necessary for the performanc e of their duties, in particular by exchanging all useful information .				
Compliance	States should			45.	Article 12:	Article 50:	
and monitoring	encourage the			Establishmen t of	Duties and Powers of	Internation al	
:	negotiation of			International	National	cooperatio	
Cooperatio	cooperation			Cooperation	Protection	n for the	
n with	agreements			Mechanisms	Authorities –	protection	
other	among			- Ibero-	Authorities	of personal	
authorities	international			American	are	<b>data</b> – In relation to	
outside the	supervisory authorities			States may adopt	responsible for	third	
framework	that			international	establishing	countries	

/ between	contribute to		cooperation	mechanisms	and	
framework	more		mechanisms,	for	internation	
	effective		which may		al	
S			include:	cooperation with the		
	cooperation		include:		organisatio	
	and		- mechanisms	personal data	ns, the	
	coordination.		that allow	protection	Commission	
	Applicable		reinforcing	authorities of	and	
	national		international	third	supervisory	
	legislation		assistance	countries.	authorities	
	may confer		and		shall take	
	powers on the		cooperation		appropriate	
	supervisory		in the		steps to:	
	authorities to		application of		(a) develop	
	authorise		relevant		internation	
	some or all		national law.		al	
	international				cooperation	
	transfers in		- assistance		mechanism	
	their		between		s to	
	jurisdiction		control		facilitate	
	before they		authorities		the	
	are carried		through		effective	
	out. Or be		notification		enforcemen	
	capable of		and		t of	
	demonstratin		submission of		legislation	
	g that the		claims,		for the	
	transfer		assistance in		protection	
	complies with		investigation		of personal	
	the		s, and		data;	
	guarantees		information		(1-)	
	provided for		exchange.		(b) provide	
	in the Madrid				internation	
					al 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.	in the enforcemen t of legislation for the protection of personal data, including through notification, complaint referral, investigativ e assistance and information exchange, subject to appropriate safeguards for the protection of personal	
			for the protection	

	T T	
		(c) engage
		relevant
		stakeholder
		s in
		discussion
		and
		activities
		aimed at
		furthering
		internation
		al
		cooperation
		in the
		enforcemen
		t of
		legislation
		for the
		protection
		of personal
		data;
		(d) promote
		the
		exchange
		and
		documentat
		ion of
		personal
		data
		protection
		legislation
		and

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

		to the			
		provisions			
		of this			
		Convent-			
		ion; and			
		b. to			
		contribute			
		actively to			
		this			
		evaluation			
		process.			
Compliance	The	Explanato	Implied in	Article 82:	
and	Responsible	ry Report:	Article 44:	Right to	
monitoring	person will be	Article 99	Restitution –	compensati	
:	liable for the	– In order	sets out a	on and	
	pecuniary and	for the	right to	liability -	
Liability	non-	Conventio	compensatio	Any	
	pecuniary	n to	n in the	controller	
	damages	guarantee	event of	involved in	
	caused to the	an	violation of	processing	
	data subjects,	effective	data	shall be	
	except if the	level of	protection	liable for	
	responsible	data	rights.	the damage	
	person can	protection	1.8	caused by	
	demonstrate	, the		processing	
	the damage is	duties of		which	
	not	the		infringes	
	attributable	controller		this	
	to him. This	and		Regulation.	
	liability is	processor		A processor	
	without	and the		shall be	
	without	and the		שומוו שכ	

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.	liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors
	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.	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	any way
sanctions	responsible
have to be	for the
effective,	event giving
proportio	rise to the
nate and	damage.
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	

				also have to be made				
				available				
				to data subjects.				
				Financial compensa tion for material and non-material damages where applicable, caused by the processing and collective actions could also be considere d.				
Compliance		Member	Additional	Article 15:	43. Claim	Article 77:	May be	
and		economies	Protocol to	Supervisor	and Sanction	Right to	possible: In	
monitoring		should	the	у	Regime –	lodge a	the event of	
:		include	Convention	authoritie	holders have	complaint	violation of	
		appropriat e remedies	for the	<b>s</b> – Each	the right to	with a	the	
		e remedies	Protection	compet-	submit claims	supervisory	provisions of	

Doto	for prives:	-£	0 to 1 to 1 to 2 to 2 to 2 to 2 to 2 to 2	before the		a the a utter.	the metional	
Data	for privacy violations –	of	ent super-			authority –	the national	
subject	could	Individuals	visory	control		Without	law	
redress	include	with regard	authority	authority to		prejudice to	implementin	
before	redress,	to	shall deal	make their		any other	g the	
supervisory	depending	Automatic	with	rights		administrati	principles,	
authorities	on the	Processing	requests	effective in		ve or	criminal or	
	system in	of Personal	and comp-	accordance		judicial	other	
	that	Data	laints	with national		remedy,	penalties	
	member	regarding	lodged by	legislation.		every data	should be	
	economy.	supervisory	data			subject	envisaged	
		authorities	subjects			shall have	together with	
		and	concer-			the right to	the	
		transborder	ning their			lodge a	appropriate	
		data flows:	data			complaint	individual	
		Autiala 4	protection			with a	remedies.	
		Article 1 –	rights and			supervisory		
		Each	shall keep			authority, in		
		supervisory	data			particular in		
		authority	subjects			the		
		shall hear	informed			Member		
		claims	of their			State of his		
		lodged by	progress.			or her		
		any person				habitual		
		concerning	Article 18			residence,		
		the	_			place of		
		protection	Assistance			work or		
		of his/her	to data			place of the		
		rights and	subjects			alleged		
		fundamenta	Each Party			infringe-		
		I freedoms	shall assist			ment if the		
		with regard	any data			data subject		
		to the	subject,			considers		
			subject,			CONSIDERS		

			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	Without	Dependent on system	May be	May be	May be	Article 79:	May be	
and monitoring	prejudice to	in the	possible: Article 10:	possible: Article 12:	possible: 43. Claim and	Right to an effective	possible: In the event of	
	any administrative	member	Sanctions	Sanctions	Sanction	judicial	violation of	
•	remedy	economy,	and	and	Regime –	remedy	the	
Data	before the	remedies	remedies –	remedies	holders have	against a	provisions of	
subject	supervisory	could include	Each Party	– Each	the right to	controller	the national	
redress in	authorities,	rights of	undertakes	Party	due process	or	law	
court	referred to	individuals	to establish	under-	of law to	processor –	implement-	
against the	above,	to pursue	appropriate	takes to	make their	Without	ing the	
controller:	including	legal	sanctions	establish	rights	prejudice to	principles,	
-	judicial	action.	and	approp-	effective in	any	criminal or	
administrat	oversight of		remedies	riate	accordance	available	other	
ive	their		for	judicial	with national	administrati	penalties	
- judicial	decisions,		violations of	and non-	legislation.	ve or non-	should be	
- Judiciai	data subjects		provisions	judicial		judicial	envisaged	
	may have a		of domestic	sanctions		remedy,	together with	
	direct		law giving	and		including	the	

recourse to	effect to	remedies	the right t	o appropriate
the courts to	the basic	for	lodge a	individual
enforce their	principles	violations	complaint	
rights under	for data	of the	with a	Terricules.
the provisions	protection.	provisions	supervisor	v
laid down in	protection.	of this	authority	<sup>y</sup>
the applicable		Conventio	pursuant	
national		n. Under	-	
		Article 9,	Article 77, each data	
legislation.		data		
			subject	
		subjects	shall have	
		have a	the right t	
		right to	an effectiv	e
		have an	judicial	
		Article 12	remedy	
		remedy	where he	or
		and to	she	
		benefit,	considers	
		whatever	that his or	
		his or her	her rights	
		nationality	under this	
		or	Regulation	
		residence,	have beer	
		from the	infringed a	S
		assistance	a result of	
		of a super-	the	
		visory	processing	
		authority	of his or h	er
		within the	personal	
		meaning	data in no	n-
		of Article	complianc	e
		15, in		

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

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

•	Additional Article 15:	e 15: Article 42.5: Article 12:	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.  Article 78: Bight to an
tl	Protocol to Supervisor the y Convention authoritie	Control and Powers of	Right to an effective judicial

monitoring	for the	s –	Authorities –	Protection	remedy
:	Protection	Decisions	gives scope	Authorities –	against a
	of	of the	for this	The sanctions	supervisory
Actions	Individuals	supervisor	according to	imposed and	authority –
against the	with regard	y author-	applicable	decisions	Each
supervisory	to	ities may	national	taken by	natural or
authorities	Automatic	be subject	legislation.	national	legal person
	Processing	to appeal		protection	shall have
	of Personal	through		authorities	the right to
	Data	the courts.		are subject to	an effective
	regarding			appeal.	judicial
	supervisory				remedy
	authorities				against a
	and				legally
	transborder				binding
	data flows:				decision of
	Article 1.4 –				a
	Decisions of				supervisory
	the				authority
	supervisory				concerning
	authorities,				them.
	which give				Each data
	rise to				subject
	complaints,				shall have
	may be				the right to
	appealed				an effective
	against				judicial
	through the				remedy
	courts.				where the
	5541.53.				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		May be	Article 15:	43. Claim	Article 12:	Administrati	May be	Article 19:
and		possible:	Supervisor	and Sanction	<b>Duties and</b>	ve fines are	possible: In	Responsibiliti
monitoring		Article 10:	У	Regime –	Powers of	available for	the event of	es –
:		Sanctions	authoritie	national	National	supervisory	violation of	Authorities
Administra		and 	s –	legislation	Protection	authorities 	the	can impose
tive fines		remedies –	supervisor	shall	Authorities –	to issue.	provisions of	administrative
		Each Party undertakes	y authoritie	establish a	National	Article 83	the national law	and financial sanctions on
		to establish	s shall	regime that allows the	protection authorities	sets out general	implementin	data
		appropriate	have	adoption of	are	conditions	g the	controllers.
		sanctions	powers to	corrective	responsible	for	principles,	
		and	issue	measures,	for imposing	imposing	criminal or	Article 20:
		remedies	decisions	and to	administrativ	such fines.	other	Sanctions
		for	with	sanction	e and		penalties	Where a data
		violations of	respect to	conducts that	monetary		should be	processor does not

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

				the basic principles for data protection.	Convention and may, in particular, impose administrative sanctions.	maximum limit and the objective criteria for establishing the relevant sanctions.	may issue warnings, temporary or permanent withdrawals of authorization s, and make decisions to discontinue, block or prohibit processing.	rative fines, and shall take all measures necessary to ensure that they are implemente d. Such penalties shall be effective, proportionate and dissuasive.	individual remedies.	
Cross- border transfers										
General principles relating to internation al transfers:	As a general rule, international transfers of personal data may be carried out when the State to which	16. A data controller remains accountab le for personal data under its control	Member economies should refrain from restricting cross- border flows between	Article 12: Transborde r flows of personal data and domestic law	Article 14: Transbord er 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 transbord er flows of personal data between itself and another country where (a) the other country substantia lly observes these Guidelines or (b) sufficient safeguards	themselves and other member economies where the other economy has in place legislative or regulatory instrument s 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 informatio n across-borders.	A Party shall not, for the sole purpose of privacy protection, prohibit/ subject to special authorisatio n 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 authorisati on transbord er 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/terri tory/sector/ activity/ international organisation/ recipient has an appropriate level of protection of personal data (acknowledg ed 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 internation al organisatio n 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 enforcem ent mechanis ms and appropriat e measures put in place by the data controller, to ensure a continuing level of protection consistent	or when a Party will transfer through the intermed- iary of another Party to a non- Contracting State.  Outside the framework: see	ting the provisions of the Conventio n or if a Party is bound by harmonise d rules of protection shared by States belonging to a regional internatio nal organisati on	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	including for onward transfers of personal data from the third country or an internation al organisatio n to another third country or to another internation al organisatio	
to ensure a mongst privacy instrume s that giv practical	framework: see additional Protocol CETS 181 – Article 2	regional internatio nal organisati on  Explanato ry Report: Article	mechanism Transfer authorised by the control	country or to another internation al	
18. Any restriction s to transbord er flows of personal data should be		There might, however, be exception al cases where there is a			

proportio	real and
proportio	
nate to	serious
the risks	risk that
presented,	this free
taking into	circulation
account	of state of the st
the	personal
sensitivity	data will
of the	lead to the
data, and	circumven
the	tion of the
purpose	provisions
and	of the
context of	Conventio
the	n. As an
processing	exception,
	this
	provision
	has to be
	interprete
	d .
	restrictivel
	y and
	Parties
	cannot
	rely on it
	in cases
	where the
	risk is
	either
	hypothetic
	nypothetic

al or
minor.
. 121
- outside
the
framewor
k
the
transfer of
personal
data may
only take
place
where an
appropriat appropriat
e 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

			cafoguarda			
			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			
		l l	J G			

				proportio nate measure in a demo- cratic society, or constit- utes necessary and proport- ionate measures in a demo- cratic society for freedom of expression .)				
Mechanism s: 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 mechanis m 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.

		data protection the former provides is in comp- liance with the provisions of this Convent- ion and, where necessary, recomme nd measures to be taken to reach such complianc	shall not require any specific authoris- ation. Elements for the Commission to take account of when assessing adequacy are specified.
		e.	
Mechanism	The Cross- Border	Article 23 36. General	
s:	Privacy	g Rules for	
Approved	Rules	The Personal	
self-	System – a	Conventio Data –	
assessment	practical	n International	
schemes	mechanism	Committe transfers can	
for	for APEC	e may take place if	
organisatio	economies to transfer	develop or the exporter	
ns	personal	approve and recipient	

		:f	-4			
		informatio	standardis	adopt a		
		n across-	ed	binding self-		
		borders.	safeguards	regulation		
			referred	scheme or an		
			to in	approved		
			Article 14.	certification		
				mechanism.		
				No such		
				schemes are		
				specified.		
Mechanism	If States do		No	36. General	Article	
s:	not afford the		specific	Rules for	46(2)(b):	
3.	level of		mention	Transferring	Transfers	
Binding	protection		of BCRs,	Personal	subject to	
Corporate	protection provided for		but <b>Article</b>	Data –	_	
Rules	· .				appropriate	
(BCRs)	in the Madrid		14.3.b.	International	safeguards	
, ,	Resolution,		suggests	transfers can	<ul><li>Personal</li></ul>	
	transfers can		that ad	take place if	data to a	
	be made		hoc or	() - Exporter	third	
	where those		approved	and recipient	country or	
	who expect to		standardis	adopt a	internation	
	transmit such		ed	binding self-	al	
	data		safeguards	regulation	organisatio	
	guarantee		provided	scheme or an	n only be	
	that the		by legally-	approved	transferred	
	recipient will		binding	certification	if	
	afford such		and	mechanism.	appropriate	
	level of		enforceabl	No specific	safeguards	
	protection. In		е	No specific	are in place.	
	particular,		instrumen	mention of	One	
	where the		ts adopted	BCRs.	specified	

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

Codes of Conduct	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.	appropriate safeguards  - Personal data to a third country or internation al organisatio n only be transferred if appropriate safeguards are in place. One specified safeguard is an
	personal data in the recipient country and the recipient proves	if appropriate safeguards are in place. One specified safeguard is

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
internation
al
organisatio
ns under
the terms
referred to

					in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitmen ts, via contractual or other legally binding instruments , to apply those appropriate safeguards including with regard to the rights of data subjects.	
Mechanism s: Contractual Clauses	If States do not afford the level of protection provided for in the Madrid		Article 14 Appropria te 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,	can be	transfers can	safeguards	
transfers can	based on	take place if	– Personal	
be made	approved	the exporter	data to a	
where those	standardis	and recipient	third	
who expect to	ed	sign	country or	
transmit such	safeguards	contractual	inter-	
data	provided	clauses/other	national	
guarantee	by legally	legal	organis-	
that the	binding	instrument	ation only	
recipient will	and	that offers	be	
afford such	enforce-	sufficient	transferred	
level of	able	guarantees.	if	
protection.	instru-	_	appropriate	
Guarantees	ments.		safeguards	
could result	This could		are in place.	
from	result in		One	
appropriate	the use of		specified	
contractual	mechan-		safeguard is	
clauses.	isms such		standard	
	as		data	
	contract-		protection	
	ual		and	
	clauses,		contractual	
	but no		clauses	
	specific			
	mechan-			
	ism is set			
	out.			
Mechanism		36. General	Article	
s:		Rules for	46(2)(f):	
		Transferring	Transfers	

Certificatio	Personal	subject to	
n	Data –	appropriate	
	International	safeguards	
	transfers can	- Personal	
	take place if	data to a	
	the exporter	third	
	and recipient	country or	
	adopt a	internation	
	binding self-	al	
	regulation	organisatio	
	scheme or an		
	approved	transferred	
	certification	if	
	mechanism.	appropriate	
	No specific	safeguards	
	mechanisms	are in place.	
	are set out.	One	
		specified	
		safeguard is	
		approved	
		certification	
		mechanism	
		pursuant to	
		Article 42	
		together	
		with	
		binding and	
		enforceable	
		commitmen	
		ts of the	
		controller	
		or	

			processor in the third country to apply the appropriate safeguards.  Article 42 sets out requirements for certification mechanism.
Mechanism s:  Administra tive arrangeme nts	No specific mention of administra tive arrangem ents, but Article 14.3.b. suggests that ad hoc or approved standardis ed 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 authorisatio n from the competent supervisory authority, the appropriate safeguards may be provided for, in

	binding and enforceable e instruments adopted and implemented by the persons involved in the transfer and further processing .   - 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 arrangement s 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 internation al 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.	
Derogation	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 authorisatio n transfers to another Party where its legislation includes specific regulations for certain data	of personal	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: Derogation s for specific situations — if no adequacy decision or appropriate safeguards apply, a number of derogations are available, such as explicit consent, performanc e of a	

the interest of	categories,	recipient	public	contract,	
the data	unless the	who is	security,	public	
subject in the	other	subject to	public health	interest,	
framework of	Party's	the	protection,	establishme	
a contractual	regulations	jurisdictio	protection of	nt, exercise	
relationship,	provide	n of	rights and	or defence	
to protect the	equivalent	another	freedoms of	of legal	
vital interests	protections;	Party to	third parties,	claims, vital	
of the data	or when a	the	and public	interests.	
subject or of	Party will	Conventio	interest		
another	transfer	n. Such a	matters.		
person, or	through the	Party may,			
when legally	intermediar	however,			
required on	y of another	do so if			
important	Party to a	there is a			
public interest	non-	real and			
grounds.	Contracting	serious			
	State.	risk that			
		the			
		transfer to			
		another			
		Party, or			
		from that			
		other			
		Party to a			
		non-Party,			
		would			
		lead to			
		circumven			
		ting the			
		provisions			
		of the			

Conventio
Conventio
n. A Party
may also
do so, if
bound by
harmonise
d rules of
protection
shared by
States
belonging
to a
regional
internatio
nal
organisati
on.
Explanato Explanato
ry Report:
Article
106
Thora
There
might,
however,
be .
exception
al cases
where
there is a
real and
serious

<u> </u>		<del>                                     </del>		<u> </u>		T	
			risk that				
			this free				
			circulation				
			of				
			personal				
			data will				
			lead to the				
			circumven				
			tion of the				
			provisions				
			of the				
			Conventio				
			n. As an				
			exception,				
			this				
			provision				
			has to be				
			interprete				
			d restrict-				
			ively and				
			Parties				
			cannot				
			rely on it				
			in cases				
			where the				
			risk is				
			either				
			hypoth-				
			etical or				
			minor.				

Onward	Parties can	Parties	Article 44:	
transfers to	derogate	can	General	
third	from the	prohibit or	principle	
countries	provision	subject to	for	
	that a Party	special	transfers –	
	shall not,	authorisati	Any	
	for the sole	on	transfer of	
	purpose of	transbord	personal	
	privacy	er data	data which	
	protection,	transfers if	are	
	prohibit/	there is a	undergoing	
	subject to	real and	processing	
	special	serious	or are	
	authorisatio	risk that	intended	
	n	the	for	
	transborder	transfer	processing	
	data flows	from the	after	
	to another	other	transfer to	
	Party,	Party to a	a third	
	when a	non-Party	country or	
	Party will	would	to an	
	transfer	lead to	internation	
	through the	circumven	al	
	intermediar	ting the	organisatio	
	y of another	provisions	n shall take	
	Party to a	of the	place only	
	non-	Convent-	if, subject	
	Contracting	ion.	to the other	
	State.	Explanato	provisions	
		ry Report:	of this	
			Regulation,	
			the	

Article	conditions
106	laid down in
	this Chapter
There	
might,	are
however,	complied
be	with by the
exception	controller
al cases	and
where	processor,
there is a	including
real and	for onward
serious	transfers of
risk that	personal
this free	data from
circulation	the third
of	country or
personal	an
data will	internation
lead to the	al
circumven	organisatio
tion of the	n to
provisions	another
of the	third
	country or
Conventio	to another
n. As an	internation
exception,	al
this	organisatio
provision	n. All
has to be	provisions
interprete	in this
d	Chapter

restrictivel	shall be	
y and	applied in	
Parties	order to	
cannot	ensure that	
rely on it	the level of	
in cases	protection	
where the	of natural	
risk is	persons	
either	guaranteed	
hypothetic	by this	
al or	Regulation	
minor.	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 41<sup>st</sup> 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.