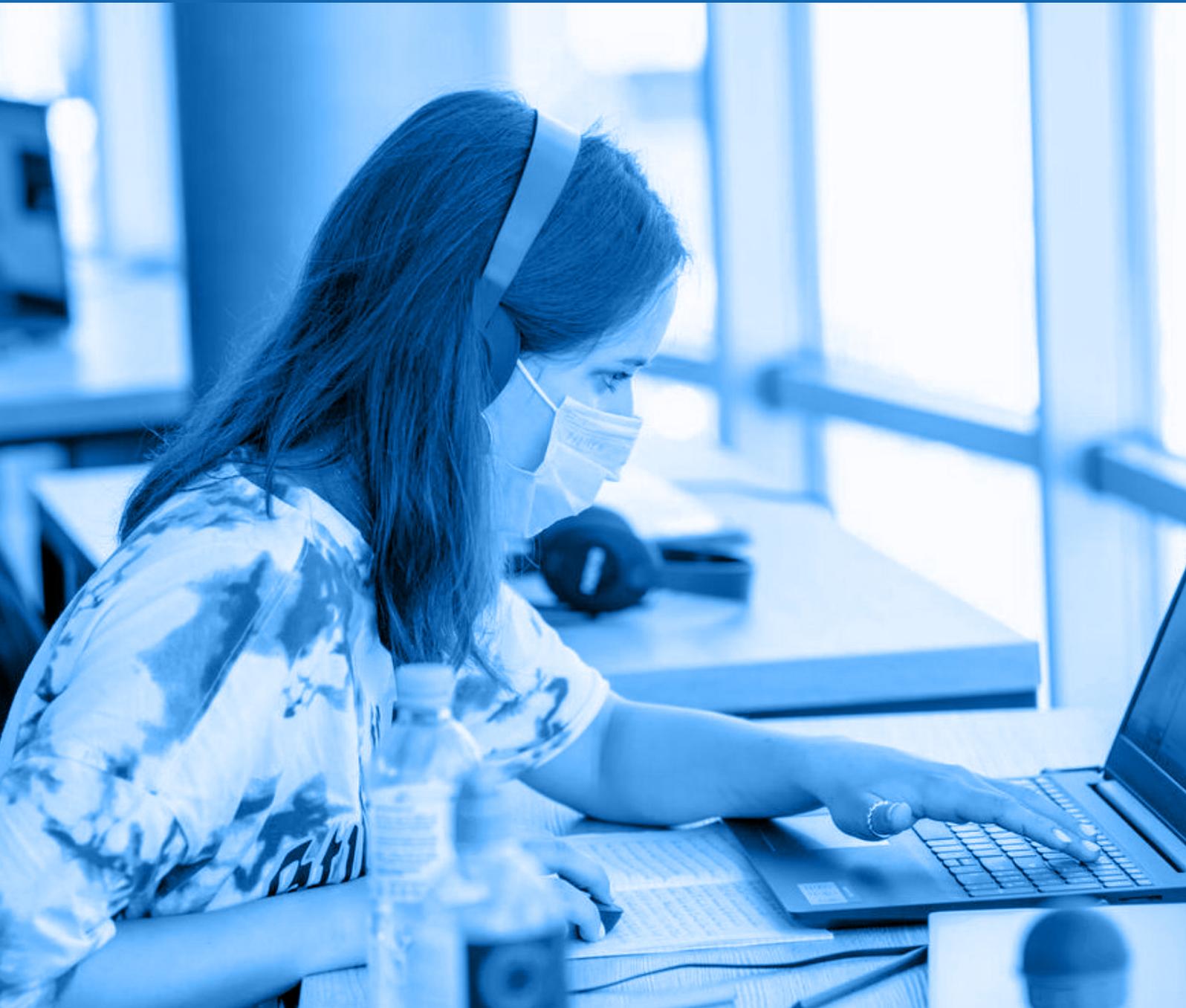




UNDP GUIDE

DRAFTING DATA PROTECTION LEGISLATION:

A Study of Regional Frameworks



CONTENTS

Acknowledgements	II
Intent and Methodology	IV
Executive Summary	VI
List of Abbreviations	XV
List of cases	XI
Introduction	1
1.1 Privacy as a core international human right	5
1.2 Privacy and the United Nations	7
1.3 Facets of the right to privacy	9
1.4 Evolution of data protection principles	10
1.5 Introduction to the Identified Regional Frameworks	12
1.6 Conclusion	16
Key Definitions	17
2.2 Personal Data and Personal Information	18
2.3 De-identification Methods	21
2.4 Data subject	25
2.5 Specific categories of data	27
2.6 Controller and Processor	31
Key considerations and summary points	34
Established data protection principles	35
3.1 Introduction	36
3.2 Fair, lawful and transparent	39
3.3 Notice and consent	42
3.4 Purpose limitation	45
3.5 Data minimisation	46
3.6 Accuracy	48
3.7 Integrity, confidentiality, and availability	49
3.8 Transparency and accountability	51
Key considerations	51
Measures for transparency and accountability	53
4.1 Introduction	54
4.2 Privacy by design	54
4.3 Information and access to personal data	59
4.4 Security safeguards	63
4.5 Reporting of personal data breach	67
4.6 Maintenance of records relating to processing activities	71
4.7 Data protection impact assessments	72
4.8 Data protection officer	76
Key considerations	78

Rights of data subjects	79
5.1 Introduction	80
5.2 The rights to access, confirmation, and information	81
5.3 The rights to rectification and erasure or deletion	87
5.4 The rights to be forgotten and to data portability	89
5.5 The rights to object and to restrict processing	93
5.6 The right against automated decision-making and profiling	95
5.7 The right to delegate (or for third-party to exercise) rights	97
5.8 Whistle-blower protection	98
5.9 General exceptions to rights of data subjects	99
Key considerations	100
Special protections for children’s data	101
6.1 Introduction	102
6.2 Current international and regional regulatory frameworks on children’s data	105
6.3 Factors and risks involved in protecting children’s personal data and online privacy	106
Key considerations	114
Data processing and access by governments	117
7.1 Introduction	118
7.2 Government access to personal data and the first principles of international human rights law	120
7.3 Exemptions governments can legitimately claim from data protection obligations	135
Key considerations	139
Regulation of Cross-Border Flows of Data	141
8.1 Introduction	142
8.2 Regulatory objectives and origins of cross-border data flows	143
8.3 Adequacy and conditions for transfer permitting cross-border data flows	146
8.4 Obligations on data controllers and accountability	150
8.5 Derogations, exceptions, and specific grounds for transfer in place of adequacy	152
8.6 Non-compliance, sanctions and penalties	155
Key considerations	160
Structure of Regulatory Authorities, Offences and Penalties	161
9.1 Introduction	162
9.2 Effective Regulatory Design	166
9.3 Structure of the Regulator	168
9.4 Functions and Powers of the Regulator	174
9.5 Penalties, remedies, and appeals	181
Key considerations	185



UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at @UNDP
One United Nations Plaza
New York, NY 10017. USA
<http://www.undp.org>

Copyright © UNDP 2023. All rights reserved.

The views expressed in this publication are those of the author(s) and do not necessarily represent those of the United Nations, including UNDP, or the UN Member States.

ACKNOWLEDGMENTS

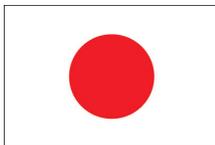
This report was authored by the Centre for Communication Governance at National Law University Delhi (CCG), with guidance from the United Nations Development Programme's (UNDP) Governance Team in the Bureau for Policy and Programme Support.

CCG is a research centre at the National Law University Delhi, one of India's premier law universities. Nine years since its foundation, the Centre continues to be India's only academic centre dedicated to researching information technology laws and policies and has globally established itself as a leading research centre on these issues. CCG undertakes academic research, provides policy input both domestically and internationally, and facilitates the capacity building of relevant stakeholders at the domestic and international levels.

Privacy and data protection have been focus areas for CCG since its inception and the Centre has helped shape discourse in this domain through research and analysis, policy inputs, capacity building, and related efforts. In 2020, the Centre launched the Privacy Law Library, a global database that tracks and summarises privacy jurisprudence emerging in courts across the world, in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. The PLL currently covers 200+ cases from 15+ jurisdictions globally and also contains a High Court Privacy Tracker that tracks emerging High Court privacy jurisprudence in India.



This guide was produced thanks to the generous support from Government of Japan, Government of Switzerland and Government of Sweden



**From
the People of Japan**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Swiss Agency for Development
and Cooperation SDC**



This material/production has been financed by the Swedish International Development Cooperation Agency, Sida. Responsibility for the content rests entirely with the creator. Sida does not necessarily share the expressed views and interpretations.

Team

The report was conceptualised by Jhalak M. Kakkar, Smitha K. Prasad, and Shashank Mohan in collaboration with UNDP. The research and drafting of the report were led by Jhalak M. Kakkar, Executive Director, CCG and Shashank Mohan, Programme Manager, CCG. The core authorship team includes Jhalak M. Kakkar, Shashank Mohan, Aishwarya Giridhar, Swati Punia, Nidhi Singh, Sangh Rakshita, Sharngan Aravindakshan, Joanne D' Cunha, Vasudev Devadasan, Akriti Gaur, and Arpitha Desai. Editors and reviewers include Jhalak M. Kakkar, Shashank Mohan, Aishwarya Giridhar, Joanne D'Cunha, Vasudev Devadasan, Akriti Gaur, Arpitha Desai, and Geetha Hariharan. Research support was provided by Bilal Mohamed, Mira Swaminathan, Priyanshi Dixit, Srishti Joshi, Aanchal Khandelwal, Aarya Pachisia, Anamika Duvaani, Anna Kallivayalil, Anushka Pandey, Avani Airan, Kunika Champawat, Raghav Ahooja, Soham Chakraborty, and Swastik Sharma.

The team would like to thank the National Law University of Delhi (NLUD) for its continued support. This report could not have been possible without the constant guidance and mentorship of the Vice Chancellor of NLUD, Prof. (Dr) Srikrishna Deva Rao. We are grateful to the Registrar of NLUD, Prof. (Dr) Harpreet Kaur for her continued encouragement and support. Special thanks is owed to Dr. Daniel Mathew, Faculty Advisor at CCG, for his steady direction and counsel.

The review process for this paper was anchored by UNDP's Risa Arai, Programme Specialist, Legal Identity, and Niall McCann, Consultant, Legal Identity, with oversight by Sarah Lister, Head of Governance. The authors would like to thank Heidi Modro for copy-editing, and Matthew Gibbons for designing this report.

Contact information

For further information on this issue, you can contact:

[Risa Arai, Programme Specialist, Legal Identity](#)
[Niall McCann, Consultant, Legal Identity](#)
[Jhalak M. Kakkar, Executive Director, CCG NLUD and Visiting Professor NLUD CCG](#)

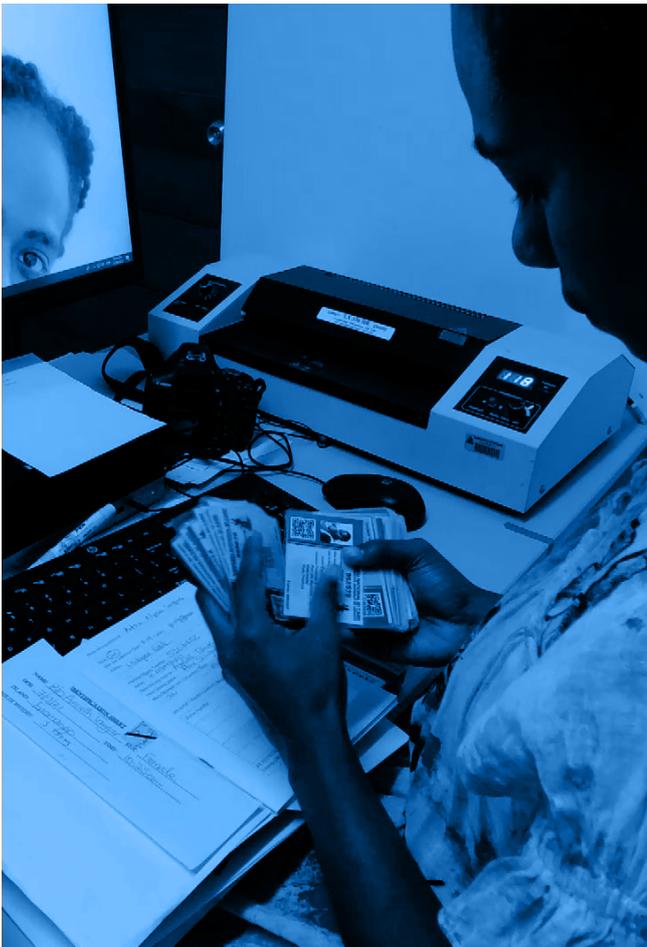
INTENT AND METHODOLOGY

Intent

This report has been drafted in the context of Target 16.9 of the Sustainable Development Goals that aims to provide “legal identity for all, including birth registration, by 2030.” Conferring proof of legal identity (via a birth certificate or a ‘foundational’ identity document such as a national ID card) to individuals is crucial in order for them to be recognised as persons before the law, enable them to exercise legal rights, and fully participate in society’s social, political, and economic systems. Providing legal identity to all involves the collection and processing of large quantities of personal data. As privacy continues to be recognised as a crucial human right around the world, the collection and processing of such data must adhere to globally established standards of data protection.

With the increase in digitisation of social and economic infrastructure, governments have expanded the use of new digital technologies in identity management schemes, to potentially enhance the delivery of public and welfare services. This shift, although with the potential to be beneficial, raises certain unique challenges from the perspective of protecting the privacy rights of individuals. Consequently, it behoves UN Member States to establish robust data protection laws and institutional frameworks when designing modern-day legal identity systems. Additionally, increased internet penetration has meant an increase in the cross-border flow of personal data for the provision of services, making data protection frameworks essential to ensure robust standards of privacy around the world.

The COVID-19 pandemic has spurred UN Member States to increase their reliance on technology as they seek to manage its effects on their populations. While technological solutions have played a significant role in the global response to the Covid-19 pandemic, they have also highlighted the prospective privacy risks that accompany digitisation, and have made the formulation of robust data protection laws and institutional frameworks more urgent. In this context, this report aims to provide UN Member States with suggested guidance on developing domestic data protection legislation, and creating a robust privacy-protecting regulatory framework.



Methodology

As this report is aimed at equipping countries with the necessary tools and context to draft privacy-protecting domestic data protection legislation, we have divided the report into various chapters covering specific themes. Each chapter contains insights that are intended to assist UN Member States in framing robust privacy-respecting regulatory frameworks. These thematic areas are based on the elements most commonly covered in a typical data protection legal framework. They include:

- definitions of key terms in data protection frameworks;
- core data protection principles;
- measures to operationalise transparency and accountability;
- data protection rights for data subjects;
- special protections for children's data;
- state exemptions from data protection obligations;
- regulation of cross-border flows of data;
- structure of regulatory authorities, and
- offences and penalties.

These components have been identified based on a comparative analysis of various regional data protection frameworks. Regional diversity has been a cornerstone of the research, and trends in data protection from the following regional data protection frameworks have been analysed:

- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework;
- the Association of South-East Asian (ASEAN) Framework;
- the African Union Convention on Cybersecurity and Personal Data Protection;
- the Commonwealth of Nations Frameworks (the Model Bill on the Protection of Personal Information, and the Model Privacy Bill);
- the Council of Europe Convention 108+;
- the European Union's General Data Protection Regulation;

- the Caribbean Community's (CARICOM) Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR);
- the Organization of American States Principles, and
- the Organisation for Economic Co-operation and Development (OECD) Guidelines.

In addition to the regional frameworks, national laws, programmes and significant case law are analysed, where relevant. Both foundational and contemporary international academic and policy literature on privacy and data protection have been drawn upon to highlight both the diversity and commonality in global approaches to data protection.

This report has been primarily written from the perspective of data protection in the context of legal identity systems, such as for birth and death registration.

In addition, the report focuses primarily on personal data processing by UN Member States, and does not comprehensively comment on the processing of personal data by private actors in the digital economy. While the report analyses the growing trend of regulating cross-border data flows between nations, it does not specifically analyse the challenges of international data sharing between countries for law enforcement and intelligence purposes. This report has also been drafted in the context of the COVID-19 pandemic and recognises and highlights the unique privacy and data protection challenges that have arisen as a result of the ongoing global health emergency.

We hope that this report provides UN Member States with a foundational framework to enable them to formulate robust data protection frameworks that safeguard individuals' privacy and human rights, as well as support the development of societal and policy goals.

EXECUTIVE SUMMARY

This report aims to guide policymakers and legislators in drafting and implementing privacy-protecting domestic data protection frameworks. The report was prepared in the context of Sustainable Development Goal (SDG) Target 16.9, which aims to provide “legal identity for all, including birth registration, by 2030.” Legal identity is central to the achievement of several other SDGs, and data generated from legal identity programmes is crucial for the measurement of over 60 other SDG targets. In addition to traditional identification systems, such as the core civil registration of births, deaths, marriages, adoptions, divorces, etc., governments are also increasingly implementing related, digitally-enhanced, identity management programmes, which often process biometric data, and which are popularly referred to as ‘digital ID’ systems. These new systems seek to enhance the efficiency of public service delivery, formulation of public policy, and monitor implementation, while leveraging advancements in digital and information technologies. By their very nature, legal identity programmes rely on the collection and processing of citizens’ and residents’ personal data. While such programmes may support the achievement of various policy goals, they also have significant implications for the privacy rights of individuals. Consequently, it is more important than ever for governments to develop identity systems that respect individuals’ right to privacy and enable effective protection of their personal data.

This report aims to help UN Member States develop domestic data protection legislation and create a robust privacy-protecting regulatory framework. It identifies key considerations and various approaches to data protection for Member States to contemplate when crafting domestic data protection laws. Over the course of different chapters, the report examines various regional data protection frameworks and explores the key elements of data protection typically covered in these frameworks. The following section briefly describes the issues covered in each chapter and summarises key concepts covered in them.

“This report aims to help UN Member States develop domestic data protection legislation and create a robust privacy-protecting regulatory framework.”

CHAPTER 1: INTRODUCTION

Several international human rights instruments recognise the right of every person to be recognised as an individual with rights before the law, via legal identity. Target 16.9 of the UN's Sustainable Development Goals — to provide legal identity for all, is primarily carried out via birth registration. In the absence of birth registration, it can also be granted via registration in national identity management programmes (such as national ID card schemes).

As global society moves towards rapid digitisation of social and economic infrastructure, nation states and private corporations collect and process more data. Such actions, however, have implications for the right to privacy, which is an internationally recognised human right. It is multi-faceted and also protects an individual's identity, autonomy, safety, and dignity. Advancements in information technology have highlighted the need for informational self-determination, and more particularly informational privacy, which may be understood as the right of individuals to control and determine how information about them is communicated to others, including State agencies. It is also a key aspect of other facets of privacy, such as bodily integrity, decisional privacy, and behavioural privacy, and is central to how the right is understood in the context of digital technology. The UN and its Member States have been instrumental in advancing the right to privacy and have included the right in landmark human rights treaties, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In 2015, the UN also designated a Special Rapporteur to examine and advance the right to privacy.

With increased digitisation, digital ID programmes are also being developed to confer legal identity to individuals. These digital ID systems involve large-scale collection and processing of personal data from citizens and residents, and can include a wide range of sensitive data, such as biometric information. This collection, processing, and use of aggregated personal and sensitive information could pose security and surveillance concerns, risks of exclusion, and stigmatisation of marginalised and vulnerable communities. The need to institute data protection laws with robust data protection principles to regulate how such data is used, therefore, has become more urgent. Comprehensive, human rights-based laws can ensure that governments provide legal identity for all its citizens and resident foreigners while ensuring individual privacy.



“The report explores the development of data protection principles across the world and how they are treated in regional and domestic frameworks”



The report explores the development of data protection principles across the world and how they are treated in regional and domestic frameworks. The development of international and regional data protection frameworks dates back to the 1970s and 1980s. Early examples of frameworks include the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980) and the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). Since then, several regional frameworks have emerged, and demonstrate the growing consensus on core data protection principles while also reflecting diversity in regional approaches. This report undertakes a comparative analysis of the following ‘Identified Regional Frameworks’:

- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework;
- the Association of Southeast Asian Nations (ASEAN) Framework on Digital Data Governance, and ASEAN Framework on Personal Data Protection;
- the African Union Convention on Cyber-Security and Personal Data Protection;
- the Commonwealth of Nations Model Bill on the Protection of Personal Information, and the Model Privacy Bill;
- the Council of Europe’s Modernised Convention on the Protection of Individuals with regards to Automated Processing of Personal Data (Convention 108+);
- the European Union’s General Data Protection Regulation (GDPR);
- the Caribbean Community’s Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR) Privacy and Data Protection Model Policy Guidelines and Legislative Text;
- the Organization of American States’ Updated Principles on Privacy and Personal Data, and;
- the Organisation for Economic Co-operation and Development (OECD) Privacy Framework.

The background and context necessary to appreciate the relevance of each of these frameworks is discussed in Chapter 1.

CHAPTER 2: DEFINITIONS OF KEY TERMS IN DATA PROTECTION FRAMEWORKS

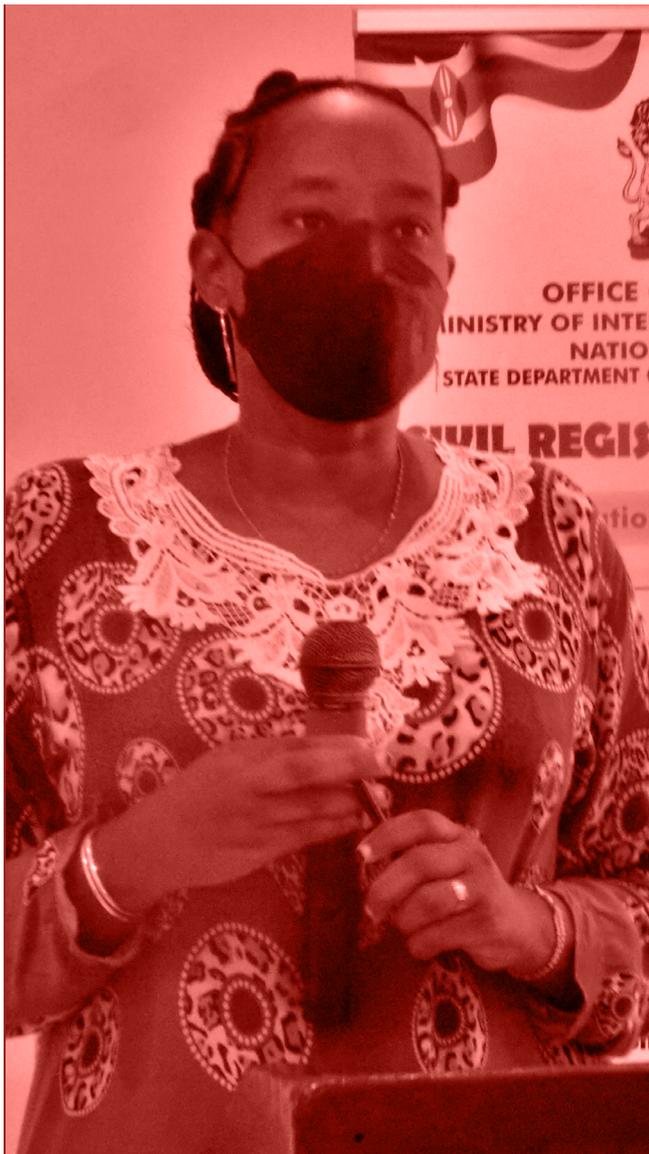
Defining key terms and concepts (e.g., personal data or data controller) reduces the ambiguity in interpreting a data protection framework and also helps delineate a framework's scope of applicability. Chapter 2 provides definitions of personal data, anonymised data, data subject, data controller, data processor, and health, biometric, and genetic data. Some of the key concepts covered in this chapter are as follows:

- Broad definition of personal data:** The processing of personal data triggers the applicability of personal data protection frameworks, and data protection frameworks apply at all stages of the data processing lifecycle. A broad definition of personal data ensures that a framework is comprehensive and future-proof, and does not exclude from its ambit any privacy-infringing uses of individuals' data. This also allows courts and regulators to protect individuals in the face of changing and ever-evolving technologies.
- High threshold for de-identification:** Because anonymised or de-identified data is subject to fewer safeguards under data protection frameworks, such frameworks should ensure that data must only be considered anonymous if it is unreasonably difficult or impossible for it to be used to re-identify individuals, otherwise known as re-identification.
- Special categories of data:** Health, biometric, and genetic data are intimately connected with an individual's identity and their use could have significant implications, such as during criminal investigations or securing health insurance. Such data is typically treated as a special category of data subject to additional safeguards.
- Public and private data controllers:** The definition of data controller should include both private organisations and public authorities, as they are the entities responsible for processing data and ensuring compliance with privacy obligations. This ensures that the framework comprehensively protects individuals from any harms arising from the processing of their personal information.



CHAPTER 3: CORE DATA PROTECTION PRINCIPLES

An analysis of the Identified Regional Frameworks reveals a shared consensus over seven data protection principles that are essential to a robust data protection framework. These principles, which are explored in Chapter 3 consist of: (i) fairness and lawfulness; (ii) notice and consent; (iii) purpose limitation, (iv) data minimisation; (v) accuracy of data; (vi) integrity, confidentiality, and availability; and (vii) transparency and accountability.



- **Fairness and lawfulness:** All processing of personal data must be undertaken for legitimate purposes and be governed by law, in line with international human rights obligations of States.
- **Notice and consent:** These principles traditionally protect the autonomy of individuals by informing them of how their personal data will be processed and allowing them to make decisions whether they consent to such processing. However, emerging scholarship also recognises that placing the onus of privacy entirely on individuals through notice and consent policies may result in compromised protection due to factors, such as ‘consent fatigue’ and power asymmetries between data subjects and data controllers.
- **Purpose limitation:** Collected data must only be used for the purposes that it was collected for, or those legitimately connected to this original purpose. This principle guards against collected data being misused later in its lifecycle for unforeseen purposes, especially in a manner that may impact individual privacy.
- **Data minimisation:** Data minimisation is one of the core data protection principles, and it calls for limiting data collection to only what is required to fulfil a specific and legitimate purpose. By mandating the collection of as little data as possible, this principle protects against excessive data aggregation and the privacy harms associated with this practice.
- **Integrity, confidentiality, and availability:** These principles impose obligations on data controllers and processors to treat individuals’ personal data with a minimum standard of care to foster information security and data protection. Adopting reasonable security safeguards mitigate against risks such as unauthorised access or use and the destruction or loss of data, among others. This protects individuals in the case when personal data records may be inaccurate or unavailable, or where their data has been accessed without authorisation.

CHAPTER 4: MEASURES TO OPERATIONALISE TRANSPARENCY AND ACCOUNTABILITY

The principles of transparency and accountability are essential to ensure the effective implementation of a data protection framework. They require data controllers and processors to comply with the data protection principles, as well as demonstrate compliance through measures such as the maintenance of records and providing information on data processing and management practices.

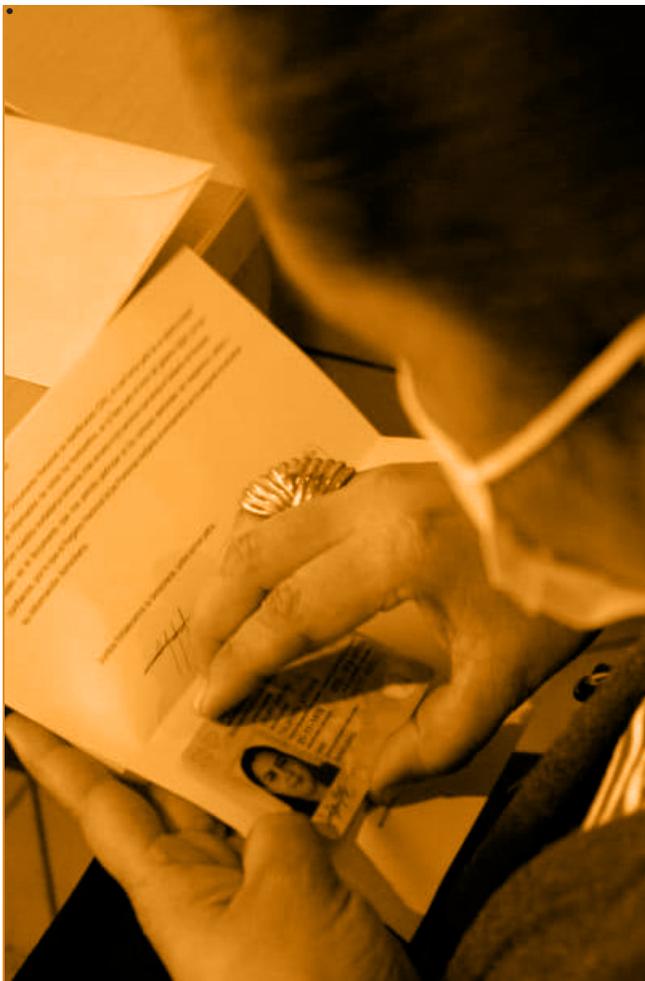
Chapter 4 discusses the measures typically required to operationalise transparency and accountability, which include: (i) adoption of privacy by design; (ii) providing data subjects access to their data and related information; (iii) imposing security safeguards for personal data; (iv) reporting data breaches; (v) maintaining records relating to data processing; (vi) carrying out data protection impact assessments; and (vii) appointing data protection officers for monitoring compliance.

Such measures are essential to ensure that a data protection regime is effective, accountable and rights-based. They also enable regulators to more effectively enforce data protection laws. In addition, these measures help data subjects obtain redress for violations of their rights due to transparency obligations imposed on controllers.

- **Privacy by design and data protection impact assessments:** Requiring privacy by design and data protection impact assessments ensures that privacy and data protection are built into the design and functioning of systems and processes. This ensures that relevant risks are accounted for based on the kinds of personal data being processed and the purposes of processing. In addition to ensuring privacy, they help foster trust in the system and data security. It is particularly important for controllers and processors to comply with objective data protection standards so that user-consent is not relied on as the sole data protection tool.
- **Transparency obligations:** Transparency obligations that require data controllers and processors to provide information on the data being collected and related information, such as purposes of processing and the intended recipients of the information, to data subjects is critical to enable data subjects to exercise their rights under data protection frameworks since they would otherwise be unaware of processing based on their personal data. Other transparency measures such as requiring notifications in case of data breaches allow individuals to mitigate privacy risks, and incentivise data controllers and processors to adopt strong data security practices.
- **Other accountability measures:** Measures such as imposing security safeguards, record maintenance obligations, and appointing data protection officers can support transparency and accountability and help the overall enforcement of the data protection framework.

CHAPTER 5: RIGHTS OF DATA SUBJECTS

Chapter 5 discusses a central pillar of data protection, the rights of data subjects. Providing comprehensive rights is crucial to empower data subjects to protect their privacy and obtain redress for data protection violations by data controllers and processors. The rights provided to data subjects operationalise privacy in the context of data protection frameworks along with the obligations imposed on data controllers and processors. Chapter 5 explores the following rights of data subjects: (i) access and confirmation of data relating to them; (ii) rectification, erasure, or deletion; (iii) the right to be forgotten; (iv) data portability; (v) object to processing; (vi) restrict processing; (vii) against automated decision making and profiling; and (viii) allow third parties to exercise data rights.



- **Rights to access and information:** The right of data subjects to know that a controller is processing their personal data and related information, such as the data being collected, the purposes of processing, and the recipients of data, and of access to the relevant information may be a necessary first step to exercising all other rights under data protection legislation. Without this information, data subjects would also be unable to meaningfully consent to the use of their personal data.
- **The right to rectification and against automated decision-making:** From the perspective of legal identity systems, the right to rectification in combination with the right to access information is likely to be among the most important rights available to data subjects. If a controller or processor has incorrect information, data subjects may be excluded from public welfare and financial services if they are not able to correct errors. The rights to rectification and the right against automated decision-making also guard against unfair or incorrect outcomes based on an individual's data. Establishing comprehensive data standards therefore ensures equal and fair treatment and safeguards human rights.
- **The right to be forgotten:** The right to be forgotten is a contemporary data protection right that enables data subjects to request that their data is erased in certain circumstances. In the digital context, this right is usually exercised to require search engines and websites to remove information from search results and webpages. The operationalisation of this right can have significant implications for access to information and the freedom of expression, and it must be carefully balanced against these factors.
- **Comprehensive data protection:** Rights, such as the right to object to or restrict processing, data portability and allowing third parties to exercise rights on behalf of data subjects support the exercise of other data protection rights and objectives, as well as provide comprehensive protection to data subjects.

CHAPTER 6: SPECIAL PROTECTIONS FOR CHILDREN'S DATA

The vulnerability of children to privacy risks highlights the need for specific protections to be built into data protection frameworks to protect children and their personal data. Children may face greater risks from both governmental and private use of their data, particularly in light of the COVID-19 pandemic, as access to education and other activities becomes more reliant on the internet. Chapter 6 discusses factors that need to be taken into consideration when regulating children's data.

- **Need for focus on children's data:** Among the Identified Regional Frameworks, only the GDPR and the OAS Principles discuss consent specific to children in the digital context. In protecting children and their personal data, data protection frameworks must account for children's varying levels of cognitive development, differing cultural contexts and socioeconomic settings. They must also balance a protectionist approach with the participatory rights of children.
- **Age of consent:** Data controllers and processors largely use consent-based privacy management tools. This may not be the best approach for children, who may be unable to truly provide informed consent. Further, data protection frameworks often prescribe a digital age of consent which does not account for the varying capacities and cognitive development of children.
- **Parental consent:** Many data protection frameworks allow for parents or guardians to provide consent on behalf of children. However, there are a few issues that can arise in this context. Firstly, this approach is dependent on the notion that parents or guardians act in the best interests of the child. This may not always be the case and can conflict with the participatory or emancipatory rights of children, which could extend to the child's right to decision-making and online expression. Secondly, parents or guardians themselves may be unaware of the privacy risks to children that could arise in the digital context.
- **Age verification:** Some forms of age verification may involve excessive collection of data that could result in further risks to children. Consequently, the sophistication of such techniques must be context and use-appropriate. Nevertheless, it can also be challenging to employ age verification mechanisms. Often simpler forms of age verification, such as provision of date of birth, can be easily manipulated. Assessing the likelihood that a child may access a platform and be exposed to the resultant risks should determine the verification methods that are employed as opposed to prescribing blanket forms of verification. Furthermore, personal data collection and processing, when it relates to children of certain age groups, should be explicitly based on opt-in policies, with no personal data being shared without explicit consent.
- **Measures to protect children's data:** It is crucial for data protection frameworks to mandate minimal collection of children's data that is strictly necessary to provide services. Additionally, data controllers can provide children with information and tools to understand potential harms in a manner that is easily comprehensible. It is also important to provide children, teachers and parents with resources to understand privacy risks and assess potential harms that may arise from the use of digital products and services.

CHAPTER 7: STATE EXEMPTIONS FROM DATA PROTECTION OBLIGATIONS

This report recognises that governments are likely to be among the largest public collectors and processors of data, and proceeds to identify the first principles applicable to government access of personal data in the context of a data protection law. Data protection frameworks provide exemptions to the state from data protection obligations for certain legitimate purposes, such as national security, maintaining public order, and undertaking criminal investigations. Chapter 7 explores the requirements that such exemptions are typically required to conform to.

- **Applicable safeguards:** Typically, under international human rights law, restrictions on core fundamental rights such as the right to privacy require the restrictions to: (i) be provided by law; (ii) not be arbitrary; (iii) pursue a legitimate aim; and (iv) be necessary and proportionate to the legitimate aim pursued. These factors aim to narrowly tailor restrictions on rights and seek to balance legitimate governmental objectives with the rights of data subjects.
- **Narrow, targeted exemptions:** It is essential for data protection principles and obligations in regulatory frameworks to apply to both the government and the private sector, especially given that the right to privacy is an internationally recognised human right. In order to have an effective data protection framework that safeguards the right to privacy, any exemptions for governments to obligations under data protection regulatory frameworks must be narrowly tailored, specific, proportional to the aims sought to be achieved, and contain robust safeguards to ensure accountability.



CHAPTER 8: REGULATION OF CROSS-BORDER FLOWS OF DATA

Provisions in data protection frameworks affecting cross-border data flows must balance the need for seamless data transfers and economic interests with the legitimate need of governments to protect the privacy of their citizens and prevent data misuse. Chapter 8 examines both geographical and organisational norms for cross-border data flows and highlights the key goal of ensuring that data controllers remain accountable to protect data as it moves across jurisdictions.

- **Objectives of regulating cross border data flows:** A key objective for regulation is to ensure that personal data that is transferred to another territory receives a comparable level of protection and security. Commercial and economic interests can also drive such regulation.
- **Adequacy requirement:** The cross-border transfer of personal data is generally dependent on an assessment of the adequacy of protection, i.e., a reasonable level of protections afforded to personal data by the receiving territory, typically being made by an independent authority in a country. There is a list of factors to consider while making an adequacy assessment which includes the nature of data, the legislative framework of the destination country, and the purpose and the duration of processing. Adequacy assessments should ideally be made by independent authorities in a transparent and consultative manner. Furthermore, assessments must also be periodically monitored.
- **Absence of adequacy:** Frameworks may have differing standards of adequacy. In the absence of adequacy or comparable safeguards, frameworks still allow for cross-border data flows by placing specific data protection obligations on data controllers through legally binding instruments, such as Standard Contractual Clauses. A self-certification mechanism which is considered adequate may also be a substitute for an adequacy assessment. However, such mechanisms can pose risks to privacy and other human rights in the absence of adequate protections in domestic law. As noted by the European Court of Justice in *Schrems v Data Protection Commissioner and Another* (Schrems I), self-certification mechanisms must be founded on state-based systems that identify and penalise infringements of privacy and data protection rights.
- **Specific grounds for transfer:** Frameworks may allow for additional grounds under which personal data may be transferred. These grounds do not operate as exemptions from the obligation to protect data, but instead provide for flexibility in certain situations, such as when explicit consent is given by the data subject, or when transfers are required for the performance of contracts, or in the case when transfers are necessary in the public interest.

CHAPTER 9: STRUCTURE OF REGULATORY AUTHORITIES, AND OFFENCES AND PENALTIE

Having a regulatory framework that can effectively enforce data protection obligations is essential to protect data subjects. While the exact design of a regulatory framework may vary depending on national legal systems and regulatory contexts, the report stresses the importance of establishing a regulatory system that can effectively enforce data protection legislation. Chapter 9 explores the regulatory frameworks found in the Identified Regional Frameworks, and considers the following factors: the components of effective regulatory design; the structure of regulators (including factors such as composition, appointment requirements, funding, etc.); functions and powers of regulators; and penalties, remedies, and appeals.

- **Independent functioning:** Ensuring the independent functioning of the relevant regulator is key to setting up any effective regulator. However, it is particularly important in the context of a data protection framework since the regulator would be required to oversee the data processing activities of both private, as well as State entities. The manner and source of funding, process for appointments and dismissals of members of the regulatory body, and assessing conflicts of interest are some measures that have been addressed in the Identified Regional Frameworks and are explored in this report.

- **Transparency and accountability:** Accountability mechanisms for regulators are important to guard against abuse of powers by the regulator and to ensure the effective implementation of the data protection framework. Measures seeking to ensure transparency, such as reporting requirements, publishing guidelines on the operation of the regulator, and undertaking public consultations can aid in creating accountability for, and engendering trust in the regulator. Measures to hold regulators accountable to multiple stakeholders, such as the public, legislature, and regulated entities can also aid in these objectives.
- **Resource allocation:** Effective enforcement of data protection frameworks relies on the regulator's ability to keep pace with upcoming technology and coordinate with various sectoral regulators. Consequently, the provision of adequate human and financial resources are likely to be extremely important for the regulator to be able to perform its functions effectively.

By analysing the foundational components of the Identified Regional Frameworks, this report aims to serve as a guide on emerging best practices in data protection laws and policy, and unpack the critical challenges faced in designing, implementing, and enforcing data protection frameworks.

LIST OF ABBREVIATIONS

Aadhaar Act, 2016 – Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act 2016 (India)

Aadhaar Amendment Act, 2019 – Aadhaar And Other Laws (Amendment) Act, 2019 (India)

Aadhaar Judgement – Justice KS Puttaswamy v Union of India (2019) 1 SCC 1 (Supreme Court of India)

African Court – African Court on Human and Peoples’ Rights

APEC – Asia-Pacific Economic Cooperation (forum)

APEC Privacy Framework – APEC Privacy Framework (2015)

ASEAN – Association of Southeast Asian Nations

ASEAN Digital Governance Framework – ASEAN Framework on Digital Data Governance (2018)

ASEAN DP Framework – ASEAN Framework on Personal Data Protection (2016)

AU Convention – African Union Convention on Cyber-Security and Personal Data Protection

BCRs – Binding Corporate Rules

CBPR – APEC Cross Border Privacy Rules

CMB – Citizenship and Migration Bureau (Estonia)

CoE – Council of Europe

Commonwealth PPI Bill –Model Bill on the Protection of Personal Information (The Commonwealth)

Commonwealth Privacy Bill –Model Privacy Bill (The Commonwealth)

Convention 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

Convention 108+ – Convention for the Protection of Individuals with regard to Processing of Personal Data (2018)

COPPA – Children’s Online Privacy Protection Act (United States)

CRC – UN Convention on the Rights of the Child

DPIA – Data Protection Impact Assessment

ECHR – European Convention on Human Rights

ECIPIE – European Centre for International Economic Policy

ECJ – European Court of Justice

ECtHR – European Court of Human Rights

EDPB – European Data Protection Board

EDPI – Estonian Data Protection Inspectorate

EDPS – European Data Protection Supervisor

EEA – European Economic Area

FIPPS – Fair Information Practice Principles

GDPR – General Data Protection Regulation (European Union)

HEW Advisory Committee – United States Department of Health, Education and Welfare Secretary’s Advisory Committee on Automated Personal Data Systems

HIPCAR Privacy Framework – Harmonization of ICT Policies, Legislation and Regulatory Procedure in the Caribbean (Privacy and Data Protection: Model Policy Guidelines & Legislative Texts)

Huduma Judgement – Nubian Rights Forum v Attorney General of Kenya and Ors [2020] eKLR, [1040] (High Court of Kenya)

IACHR – Inter-American Court of Human Rights

ICCPR – International Convention on Civil and Political Rights

ICT – Information and Communications Technology

Identified Regional Frameworks -

Indian Privacy Judgement – Justice KS Puttaswamy v Union of India (2017) 1 SCC 1 (Supreme Court of India)

IPRS – Integrated Population Registration System (Kenya)
ISP – Internet Service Provider
Johannesburg Principles – Johannesburg Principles on National Security, Freedom of Expression and Access to Information
Katiba Judgement – Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology, Ex Parte Katiba Institute & another [2021] eKLR, 22 (High Court of Kenya)
LED – European Union Law Enforcement Directive
MLATs – Mutual Legal Assistance Treaties
MNIC – Multipurpose National Identity Card (India)
NIIMS Rules – Registration of Persons (National Integrated Identity Management System) Rules, 2020 (Kenya)
NIMS – National Integrated Identity Management System (Kenya)
OAS – Organization of American States
OAS Principles – Proposed Statement of Principles for Privacy and Personal Data Protection in the Americas by the Inter-American Juridical Committee (26 March 2015)
OECD – Organisation of Economic Cooperation and Development
OECD Guidelines – OECD Privacy Framework Booklet (2013)
Ofcom – Office of Communications, United Kingdom
PAN – Permanent Account Number (India)
PIC – Personal Identification Code (Estonia)
PII – Personally identifiable information
PR – Population Register (Estonia)
RPA – Registrations of Persons Act (Kenya)
SCCs – Standard Contractual Clauses
Schrems I – Schrems v Data Protection Commissioner and Another Case C-362/14 (European Court of Justice)
Schrems II – Data Protection Commissioner v Facebook Ireland and Maximillian Schrems Case C-311/18 (European Court of Justice)
Siracusa Principles – Siracusa Principles on the Limitation and Derogation Provisions in the International Convention on Civil and Political Rights
UDHR – Universal Declaration of Human Rights
UIDAI – Unique Identification Development Authority of India
UK ICO – United Kingdom Information Commissioner’s Office
UN – United Nations
UN Legal Identity Task Force – UN Legal Identity Agenda Task Force
SDGs – Sustainable Development Goals
UNHRC – UN Human Rights Council
UNICEF – UN International Children’s Emergency Fund
VID – Alternative Virtual Identity (India)

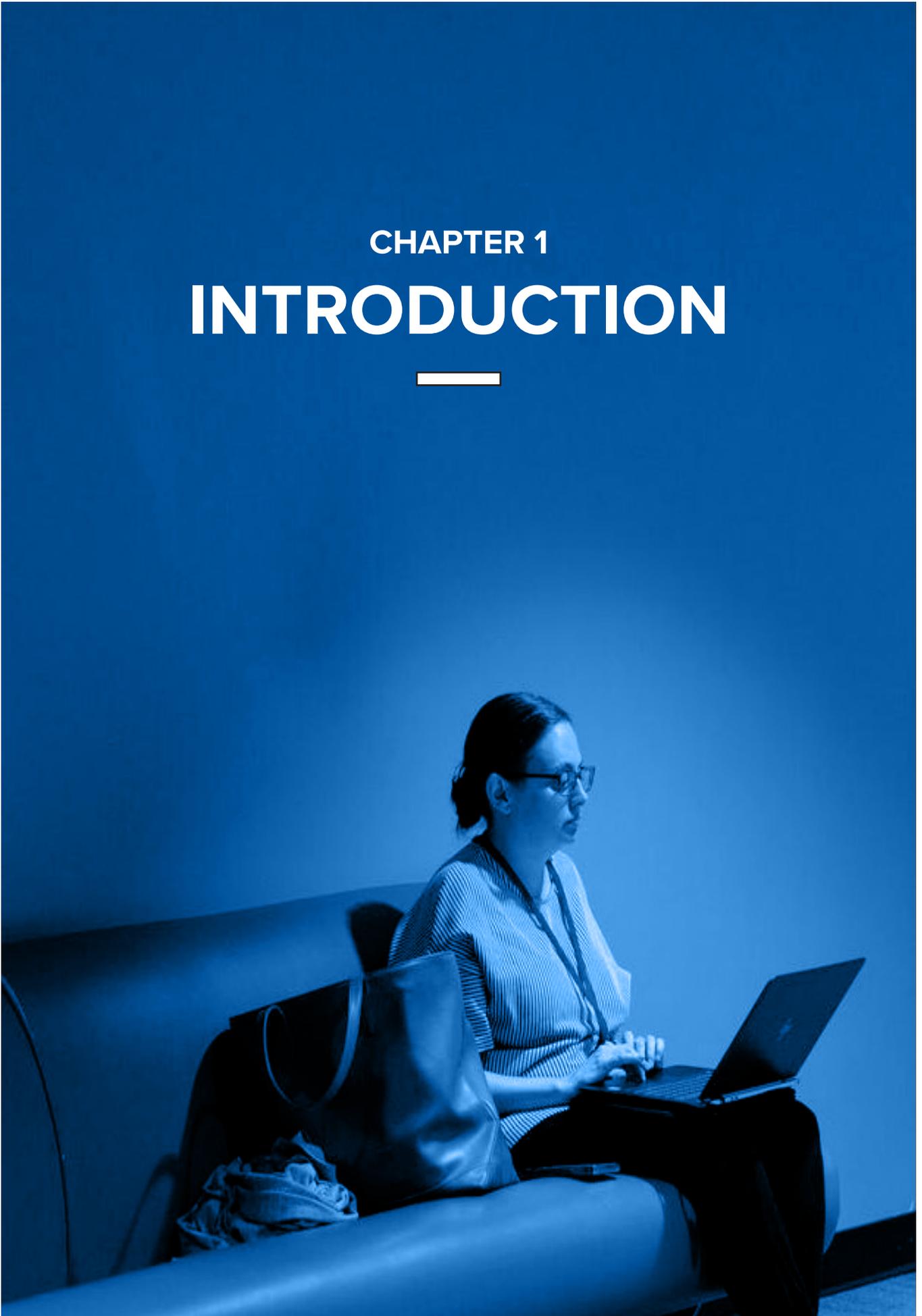
LIST OF CASES

1. *Antonius Cornelis Van Hulst v Netherlands* Communication No. 903/1999
2. *Ben Faiza v. France*, Application no. 31446/12, (ECHR 2018)
3. *Benedik v. Slovenia*, Application No 62357/14
4. *Big Brother Watch and Others v. The United Kingdom*, (2015) Applications nos. 58170/13, 62322/14 and 24960/15).
5. BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07
6. Case C-131/12 *Google Spain v AEPD* [2014] OJ C 212
7. Case C-136/17 *GC and Others v CNIL* [2019] ECLI:EU:C:2019:773
8. Case C-201/14 *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others* [2015] ECLI:EU:C:2015:638
9. Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd*, Maximillian Schrems [2020] ECLI:EU:C:2020:559.
10. Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] EU:C:2015:650;
11. Case C-40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* decision dated 29 July [2019] ECLI:EU:C:2018:1039
12. Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:15
13. Case C-518/07 *European Commission v Federal Republic of Germany* [2010] OJ C113/3
14. Case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2009] E.C.R. I-03889
15. Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, 1–2 (Oct. 19, 2016)
16. Case C-614/10 *European Commission v Republic of Austria* [2012] OJ L281/31
17. *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, (2015) Case C-311/18
18. *Entick v Carrington* 1558-1774 All E.R. Rep. 45; *Boyd v United States* 116 U.S. 616.
19. *Esbester v. The United Kingdom*, European Commission of Human Rights, Application No. 18601/91.
20. *Escher v Brazil* IACHR (ser. C) No. 200/2009
21. *Fontevecchia and D’amico v. Argentina* Am. Ct. H.R. (ser. C) No. 238/2011
22. *G v Australia* (2017), CCPR/C/119/D/2171/2012.
23. *In Re Sony BMG Music Entertainment*, US FTC Matter 062-3019 (29 June 2007) Complaint.
24. *Justice K. S. Puttaswamy (Retd.) v. Union of India and Ors.* (2017) 10 SCC 1
25. *Kennedy v United Kingdom* [2010] ECHR 682 (18 May 2010)
26. *Klass and Others v. Germany, Liberty and Others v. the United Kingdom*, Application No 58243/00, 1 July 2008
27. *Leander v. Sweden*, IHRL 69 (ECHR 1987)
28. *Malone v United Kingdom* (1984) 7 EHRR 14
29. *Minister of Police v Grace Nomazizi Kunjana* [2016] ZACC 21 (South Africa)
30. *Nubian Human Rights Forum and Ors. v The Hon. Attorney General and Ors.*, Petition 56, 58, and 59 of 2019 (Consolidated), (2020) eKLR
31. *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others* (Interested Parties) [2020]
32. *Okoiti v. Communications Authority of Kenya* Constitutional Petition no.53 of 2017 [2018] eKLR
33. *Peck v United Kingdom* (2003) 36 EHRR 41
34. *PG and JH v The United Kingdom* (2001) App no. 44787/98, ECHR 2001 IX.
35. *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Ex Parte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party)* [2021] eKLR, 22
36. *Rev. Christopher R. Mtikila v. Tanzania* Application No. 009/2011
37. *Roman Zakharov v. Russia*, Application No. 47143/06
38. *Rotaru v Romania* ECHR 2000-V, App No 28341/95
39. *S and Marper v United Kingdom* (2004)ECHR 1581, Application no. 30562/04 and 30566/04

40. *Satakunnan Markkinaporssi Oy v Finland*, App no 931/13 ECtHR (27 June 2017)
41. *Shimovolos v. Russia*, (2011) ECHR 987
42. *Silver and others v. the United Kingdom*, (1983) 5 EHRR 347, paras. 85-86
43. *Smith and Grady v The United Kingdom* (1999) 29 EHRR 493.
44. *Sri Vasunathan v The Registrar General* WP 62038/2016
45. *Subhranshu Rout @ Gugul v. State of Odisha* BLAPL No 4592 of 2020
46. *Tanganyika Law Society and the Legal and Human Rights Centre v. Tanzania*, Application No. 011/2011
47. *Toonen v Australia*, Communication No. 488/1992, (1994) UN Doc CCPR/C/50/D/488/1992
48. *Tristán Donoso v Panamá* (2009 IHRL 3064 (IACHR 2009
49. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16 decision dated 5 June 2018.
50. *Uzun v. Germany*, Application No. 35623/05, (ECHR 2010)
51. *Weber and Saravia v. Germany*, Application no. 54934/00, (ECHR 2006)
52. *Zulfiqar Ahman Khan v Quintillion Business Media* [2019] (175) DRJ 660

CHAPTER 1

INTRODUCTION



The digital revolution has opened new gateways to human development, but also raised novel human rights challenges. As social and economic activities increasingly shift online, there has been a greater focus on the need to protect personal data and privacy rights through the adoption of national legislation, the expansion of fundamental rights, and the formulation of international and regional norms.

Several international human rights instruments recognise the right of every person to be recognised as an individual with rights before the law (i.e., possess legal identity), including the right to registration at birth. As per the official UN ECOSOC-approved working definition, legal identity is granted via birth registration. In the absence of birth registration, legal identity can be conferred by a legally-mandated identity authority (such as, for example, a ‘unique identity authority’ or a ‘national registration bureau’, managing a national identity management programme, such as a national ID card scheme). The conferral of legal identity ensures that individuals are recognised by the law, helping secure the rights and benefits that are guaranteed to them by law. Universal birth registration is essential to ensure that unregistered and uncounted children are not left stateless and unable to access justice systems, as well as their basic human rights.¹ To ensure that these rights are operationalised, the 2030 Agenda for Sustainable Development established a specific target within the Sustainable Development Goals (SDGs), Target 16.9, which aims to provide “legal identity for all, including birth registration, by 2030.” Data generated from legal identity programmes is necessary to measure over 60 SDG indicators. Furthermore, experts recognise that legal identity systems help improve public policy formulation, their

implementation, the monitoring of outcomes and the better delivery of services.² Inclusive legal identity systems help tackle systemic discrimination and exclusion and are essential for the realisation of the larger ambition of the SDG’s ‘Leaving No-One Behind’ agenda.³

In the recent past, legal identity initiatives (particularly in the ‘identity management domain’ such as via national ID card schemes) have increasingly incorporated the use of technology as a consequence of an overall move toward digitisation. Estonia, The Gambia, India, Indonesia, Mexico, Iceland, Norway, and Kenya are examples of countries that have introduced (or are in the process of adopting) digital legal identity programmes (shortened to ‘digital ID’ hereafter). Digital ID systems are also being used to confer legal identity to adults who have no record of their birth registration. The Principles on Identification for Sustainable Development acknowledge that modern day identification systems use digital forms of credentials to access both public and private services through automated authentication.⁴ Most recently, and of particular interest from a human rights perspective, digital ID systems are being used in some countries to address COVID-19 public health concerns.⁵ Such systems are relying on digital ID to provide access to benefits and services to carry out contact tracing, and

1 UN Office of the High Commissioner for Human Rights, ‘Input from a child rights perspective to the United Nations High-level Political Forum on Sustainable Development’, (July 2019) https://sustainabledevelopment.un.org/content/documents/24291OHCHR_ChildRightsReport_HLPF_July19.pdf.

2 Mia Harbitz and Maria del Carmen Tamargo, ‘The Significance of Legal Identity in Situations of Poverty and Social Exclusion’ (Inter-American Development Bank, 2009), <https://publications.iadb.org/publications/english/document/The-Significance-of-Legal-Identity-in-Situations-of-Poverty-and-Social-Exclusion-The-Link-between-Gender-Ethnicity-and-Legal-Identity.pdf>

3 Bronwen Manby, ‘Legal identity for all and childhood statelessness’ (Institute on Statelessness and Inclusion) <http://children.worldsstateless.org/3/childhood-statelessness-and-the-sustainable-development-agenda/legal-identity-for-all-and-childhood-statelessness.html>.

4 World Bank, ‘Principles on Identification for Sustainable Development: Toward the Digital Age’ (February 2021) <https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf>.

5 Joseph Cannataci, Report of the Special Rapporteur on the right to privacy, A/75/147, July 2020 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/195/60/PDF/N2019560.pdf?OpenElement>

even for the provision of COVID-19 vaccine certificates. Jamaica, for instance, considered accelerating the implementation of its National Identification System to provide individualised aid and benefits to combat the effects of the pandemic.⁶ In some cases, the process of providing public and private services is also accomplished through the use of digital biometric identification technology.⁷ A 2013 survey by the Centre for Global Development pointed to 160 identification programmes worldwide that have relied on biometric identification for economic, political, and social purposes in developing countries.⁸

An area of examination, and often conflict, is between legal identity and the associated privacy challenges. The right of every person to be recognised as a person before the law involves the collection and processing of personal data by state actors. Risks to personal data may occur as a consequence of the large-scale collection and processing of data by any identification system, particularly, in a digital identification system. Such systems involve the storage of aggregated personal information and biometrics in a single place, which could pose security concerns. These concerns could involve data and storage related risks, such as security breaches leading to identity theft, unauthorised disclosure, or challenges from maintaining inaccurate data on an individual.⁹ As digital ID systems involve extensive collecting and processing of personal and sensitive personal data, such systems could be exposed to surveillance risks, or threats of data being shared beyond purposes for which it was originally collected. Additionally, digital ID systems extensively rely on technological solutions that may have inherent error rates, which may result in limiting access to these systems for certain vulnerable citizens. Without adequate safeguards to protect against these risks, such digital ID systems may run risks of exclusion, that may have an especially onerous

impact on marginalised communities and vulnerable groups. Governments and related institutions, for instance, may sometimes enter into agreements with commercial partners to manage and/or build digital ID systems.¹⁰ Privacy concerns may be exacerbated with the involvement of such private entities, particularly, if there is little clarity and transparency on their specific engagement.

Furthermore, some types of data, such as biometric or genetic data or health data, merit a higher level of protection, as it is more sensitive in nature. Processing and sharing of such data without adequate data protection measures in place could result in greater risks to an individual's rights and freedoms. Data protection concerns may be exacerbated not only due to digitisation, but also due to the inclusion of biometric identifiers, which may separately raise unique issues. While the use of biometrics can aid in facilitating social and economic development by bridging information gaps to improve access to public services or to combat fraud, it is accompanied by a necessary sharing of such sensitive personal data. Through biometrics, the identity of an individual is authenticated using biometric records stored in a database. With a common biometric identifier, an individual's identity can be linked across various accessible databases and may lead to greater privacy risks to a person and even groups of people. Responsible processing of personal data may or may not be explicitly outlined in domestic legal identity laws, which might add to privacy risks.

Given the sensitive nature of the data collected, processed, shared and stored in the operation of legal identification systems, it may be necessary to have in place robust data protection legislation that incorporate relevant data protection principles to regulate how such data is used.¹¹ These principles

6 'Jamaica fast-tracks national ID system to help distribute aid and benefits' (Privacy International, March 2020), <https://privacyinternational.org/examples/3627/jamaica-fast-tracks-national-id-system-help-distribute-aid-and-benefits>.

7 While biometric data has been captured, particularly in the law enforcement context, for many decades (e.g. via ink fingerprinting), it is the capturing and processing of digital biometric data that has raised privacy concerns, particularly as such data can be used to identify individuals across large databases, often times without their consent.

8 Many countries have begun or are in the process of implementing country wide systems that rely on biometric identification to form the basis of their national identity and civil registration projects; Gelb and Clark, 'Identification for Development: The Biometrics Revolution', Centre for Global Development Working Paper, pg. 315, https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf.

9 Julia Clark and Conrad Daly, 'Digital ID and the Data Protection Challenge' (October 2019) <https://openknowledge.worldbank.org/bitstream/handle/10986/32629/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf?sequence=1&isAllowed=y>

10 The Engine Room, 'Understanding the Lived Effects of Digital ID: A Multi-Country Study', (January 2020), https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf.

11 UN Legal Identity Agenda Task Force, 'Implementation of the United Nations Legal Identity Agenda: UN Country Team Operational

are discussed in greater detail in Chapter 3 (Data Protection Principles). It is important for legal identity laws to include data protection principles. Purpose limitation, for instance, can necessitate clarity in the scope of the legal identity programme and its data operations.¹² Ensuring that only relevant data is collected to fulfil a specific and legitimate purpose, through the principle of data minimisation, may aid in avoiding excessive collection and could mitigate privacy risks. Transparency and accountability are principles within data protection law that involve measures such as privacy by design, or establishing security safeguards to avoid breaches, all of which may be vital for digital identification systems. With such safeguards in place, it would also allow for greater transparency of private entity involvement in processes related to digital ID systems.

These concerns have also been consistently raised and addressed by the UN's Legal Identity Agenda Task Force, which has emphasised the importance of protecting individuals' personal data and that conferring legal identity should not compromise a person's privacy. In order to solve some of these challenges across jurisdictions, the Task Force, in the UN Country Team Operational Guidelines, highlight the indispensable role of strong legal, institutional, and technical safeguards within a comprehensive data protection legislation so as to provide legal identity while safeguarding privacy.¹³ The guidelines also recognise the above principles and highlight that it is crucial to have legitimate objectives when developing and maintaining a legal identity system due to the sensitive and highly personal nature of the information collected, processed, used, and shared. The Task Force notes that Member States must ensure that only necessary and proportional means are used to achieve such objectives. The Task Force emphasises that all Member States, therefore, should adopt data protection and privacy frameworks to regulate how identity data is used and protected by the state.

On the international stage, several regional inter-governmental organisations have developed data

protection or regulatory frameworks that aim to address the challenges of evolving technology. Creating regional or international frameworks that harmonise privacy and data protection laws at the national level supports the free flow of data across borders without legal or regulatory hurdles. These laws also help to foster improved personal data governance by creating specific duties for data controllers, the entities that collect and process personal data, and guarantee protections for data subjects and the individuals to whom the personal data belongs. In this context, the term 'personal data' includes all information relating to an identified or identifiable natural person.

Various regional and national data protection frameworks seek to guarantee the privacy of individuals. Different jurisdictions have several levels of privacy protection. Some countries, for example, may only permit data collection and processing for legislatively sanctioned purposes, while others may strictly regulate the cross-border flow of personal data. There is currently no global international normative treaty on data protection, despite privacy being recognised as a human right in several national constitutions. Consequently, this chapter explores the evolution of the right to privacy as an international human right, its relationship with informational privacy and data protection, and outlines the evolution of global data protection principles. It introduces the key regional frameworks that will be examined in this report.

Guidelines' (May 2020) paras 83, 86, <https://unstats.un.org/legal-identity-agenda/documents/UNCT-Guidelines.pdf>.

12 Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2 April 2013) WP 203, 4 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

13 UN Legal Identity Agenda Task Force, 'UN Strategy for Legal Identity for All' (June 2019), para 26 <https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf>; UN Legal Identity Agenda Task Force, 'Implementation of the United Nations Legal Identity Agenda: UN Country Team Operational Guidelines' (May 2020) paras 83, 86, <https://unstats.un.org/legal-identity-agenda/documents/UNCT-Guidelines.pdf>.

1.1 Privacy as a core international human right



One of the first articulations of a right to privacy was a law review article authored by Samuel D. Warren and the future United States Supreme Court Justice, Louis D. Brandeis, in 1890.¹⁴ Warren and Brandeis argued that protecting privacy requires the recognition of emotional harms and of the right to be left alone. The right to privacy has since obtained a definitive international and legal character. In 1948, the UN General Assembly adopted the Universal Declaration of Human Rights (UDHR) which states in Article 12 that “No one shall be subjected to arbitrary interference

with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.” The International Covenant on Civil and Political Rights (ICCPR), adopted in 1966 and since ratified by over 170 UN Member States, guaranteed the right against arbitrary and unlawful interference with the right to privacy.¹⁵ In its interpretative guidance to the ICCPR, the UN Human Rights Committee has stated that only relevant and competent national authorities should be able to access information regarding an individual’s private life, and only in the interests of society.¹⁶

14 Warren and Brandeis, 'The Right to Privacy', (1890), Harvard Law Review, https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

15 UN General Assembly, ICCPR, 16 December 1966, UN Treaty Series, vol. 999, page 171 Art 17.

16 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 7, <https://www.refworld.org/docid/453883f922.html>.

The Human Rights Committee's guidance also requires national legislation to state:

- the exact circumstances when interferences with privacy are permitted;
- that correspondence shall remain confidential and not be intercepted, and;
- that surveillance of communications must be prohibited.

The European Convention on Human Rights (ECHR) was adopted in 1950 and became one of the first regional instruments that recognised the right to privacy. Drafting was influenced by the then recently adopted UDHR, and the recommendations of the International Committee of the Movement for European Unity. Unlike the UDHR and ICCPR, the ECHR does not use the umbrella term 'privacy'. However, Article 8 of the ECHR, which protects the right to private and family life, home, and correspondence, has been interpreted by courts as a clause that guarantees a broader right to privacy.¹⁷ Over time, this right was expanded to incorporate various facets of privacy. The European Court of Human Rights (ECtHR) has provided an expansive definition to private and family life, which covers sexual orientation and autonomy, informational privacy in relation to collecting individuals' data, covert surveillance by the state, and bodily integrity.¹⁸

The constitutional right to privacy guaranteed by states typically covered specific aspects of privacy, such as the right against unlawful search and seizure, protection of private property, and the inviolability of home and correspondence. Since the adoption of the UDHR and ECHR, states have adopted laws protecting the right to privacy in different ways. Some states have created explicit guarantees protecting the right to privacy in their national constitutions.¹⁹ However, the type and extent of protection granted varies. Several

national constitutions provide a minimum standard of privacy protection that includes the inviolability of the home and secrecy of communications.²⁰ Where not expressly guaranteed by the constitution, courts have sometimes ruled that the right to privacy is part of other constitutionally enumerated rights, such as the right to life and personal liberty.²¹

Today, privacy is understood as a crucial right, necessary for the enjoyment of other fundamental rights and freedoms. The right to privacy encompasses several cognate rights, such as the right to protect a person's intimacy, identity, name, gender, honour, dignity, appearance, feelings and sexual orientation. Professor Alan Westin initially conceptualised privacy as an individual right and defined privacy as control over personal information.²² It has since evolved to include broader concepts like collective privacy.

The initial conception of privacy as a right to be left alone without any interference with a person's bodily autonomy and property has given way to a more nuanced understanding as a result of modern realities. With the rapid increase in the evolution and adoption of technology, more and more of our day-to-day activities now occur electronically. The increase in the generation of data by and about individuals has led to an increased focus on protecting informational privacy. Informational privacy can be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."²³ The protection of informational privacy, often through data protection laws, has become a key focus of international, regional, and domestic levels of governance.

17 Satakunnan Markkinaporssi Oy v Finland, App no 931/13 ECtHR (27 June 2017).

18 Smith and Grady v The United Kingdom (1999) 29 EHRR 493 <https://privacylibrary.ccg.nlud.org/case/smith-and-grady-vs-the-united-kingdom?searchuniqueid=238652>; Rotaru v Romania ECHR 2000-V, App No 28341/95 <https://privacylibrary.ccg.nlud.org/case/rotaru-vs-romania?searchuniqueid=310832>; PG and JH v The United Kingdom App no. 44787/98, ECHR 2001 IX <https://privacylibrary.ccg.nlud.org/case/pg-and-jh-v-the-united-kingdom?searchuniqueid=817039>; S and Marper v United Kingdom ECHR 1581, Application no. 30562/04 and 30566/04 <https://privacylibrary.ccg.nlud.org/case/s-and-marper-vs-united-kingdom?searchuniqueid=483790>.

19 Art 14 of the Constitution of the Republic of South Africa.

20 Article 10 of the Constitution of Finland; Article 18(2) of the Constitution of Ghana; Article II.2 of the Constitution of Philippines.

21 Justice K S Puttaswamy v Union of India AIR 2017 SC 4161 (India) <https://privacylibrary.ccg.nlud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uo-i-and-ors?searchuniqueid=504175>.

22 Alan F Westin, 'Privacy and Freedom' (1968), Wash. and Lee Law Review 166 <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>.

23 Alan F Westin, *ibid*.

1.2 Privacy and the United Nations

The right to privacy has been codified by several international and regional bodies over the last two decades. The regional privacy and data protection jurisprudence is vast and contains both binding and non-binding legal instruments. The UN has made significant international contributions to the development of the field of data protection and privacy. This includes reporting by the High Commissioner for Human Rights, as well as the reports submitted by the Special Rapporteurs on the Freedom of Expression, Counter Terrorism and Xenophobia. Several UN agencies have also contributed to the debate on the right to privacy and data protection, including the UN Human Rights Committee,²⁴ the UN Development Group,²⁵ the UN General Assembly²⁶ and the UN Legal Identity Agenda Task Force.²⁷

In 1988, the UN Economic and Social Council published guidelines for the regulation of computerised data files which recognised that the computerisation of personal data had implications for individuals' right to privacy and might also threaten other freedoms.²⁸ These guidelines articulated broad principles such as fairness, non-discrimination and purpose-specification for the use of data that could be used by Member States to frame national legislations for the collection of data. The 'contours' of the right to privacy were subsequently defined even more broadly by the UN. In 2013, UN Special Rapporteur Frank La Rue described the concept of privacy as the availability of "[an] area of autonomous development, interaction and liberty, a "private sphere" with or without

interaction with others, free from state intervention and from excessive unsolicited intervention by other uninvited individuals."²⁹



- 24 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6624_E.doc.
- 25 'Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda' (United Nations Development Group) https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.
- 26 UN General Assembly, 'Resolution adopted by the General Assembly on 18 December 2013', UN A/RES/68/167 <https://undocs.org/A/RES/68/167>.
- 27 'Maintaining Civil Registration and Vital Statistics during the COVID-19 pandemic' (United Nations Legal Identity Agenda Task Force, 9 April 2020), <https://unstats.un.org/legal-identity-agenda/documents/COVID-19-Guidelines.pdf>.
- 28 Louis Joinet, 'Guidelines for the regulation of computerized personal data files' (UN Economic and Social Council, 21 July 1988) para 7 <https://digitallibrary.un.org/record/43365?ln=en>.
- 29 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, April 2013 https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

UN Member States have periodically adopted resolutions recognising and reaffirming the right to privacy in the digital age. The UN General Assembly adopted resolution 68/167, explicitly affirming that “the same rights that people have offline must also be protected online, including the right to privacy.”³⁰ The increase in information and communications technology has allowed more people to participate in global discourse, express their opinions and has fostered democratic participation. As noted by the UN High Commissioner for Human Rights, however, technology has also allowed governments, enterprises, and individuals to conduct surveillance and intercept and collect personal data.³¹

In 2015, the United Nations Human Rights Council (UNHRC) appointed a Special Rapporteur on the Right to Privacy,³² with a dedicated mandate to promote and protect the right to privacy. The Special Rapporteur has advanced the discourse on privacy, addressing issues such as governmental surveillance activities, big data and open data, privacy and technology from a gender perspective, the protection and use of health-related data, the business use of personal data, and the privacy dimensions of the COVID-19 pandemic.³³ In 2019, the Special Rapporteur for the Right to Privacy noted that while many Member States unequivocally committed themselves to international instruments which uphold the right to privacy, they act in direct contravention of such obligations by employing new technologies that are incompatible with the right to privacy.³⁴

“UN Member States have periodically adopted resolutions recognising and reaffirming the right to privacy in the digital age”

30 UN General Assembly, 'The Right To Privacy In The Digital Age' UN Doc A/RES/68/167 (Dec 2013) <https://undocs.org/A/RES/68/167>.

31 Report of the High Commissioner for Human Rights, 'The Right To Privacy In The Digital Age' (2014) A/HRC/27/37 https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

32 UN Human Rights Council (A/HRC/RES/28/16, April 2015) <https://undocs.org/A/HRC/RES/28/16>

33 United Nations Human Rights Special Procedures, Special Rapporteur on the right to privacy, <https://www.ohchr.org/en/special-procedures/sr-privacy>.

34 Report of the Special Rapporteur on the right to privacy, A/HRC/40/63 (16 October 2019), <https://undocs.org/A/HRC/40/63>.

1.3 Facets of the right to privacy

The definition of privacy differs based on different cultures and legal systems, and there is no universally accepted definition. However, several scholars have discussed the various facets of privacy, all of which come together to form the right to privacy which regional and international actors seek to protect. In 1992, Roger Clarke developed what was then considered an updated typology of the types of privacy, which could keep pace with technological developments. He proposed four dimensions of privacy, namely privacy of the person, privacy of personal behaviour, privacy of personal communication, and privacy of data.³⁵ In 2015, he added another dimension to privacy, namely the privacy of personal experience, which was in response to the widespread use of the internet and mobile media.³⁶ Another famous classification comes from Anita Allen's scholarship on unpopular privacy, which bases the classification of privacy on moral and social values.³⁷ These are:

- physical or spatial privacy – expectations of privacy around a person's home;
- informational privacy – a broad concept that includes information about the person and their communications;
- decisional privacy – the right of individuals to make personal choices about their lives free from governmental interference;
- proprietary privacy – a person's right to their reputation;
- associational privacy – relates to groups and their internal relationships, including their values and criteria for inclusion or exclusion.

One of the more recent models of privacy proposed by Koops *et al* puts forth a different model.³⁸ They identify eight types of privacy: bodily privacy, spatial privacy, communicational privacy, proprietary privacy, intellectual privacy, decisional privacy, associational privacy, and behavioural privacy. Informational privacy is a key aspect of each of these eight facets and is also central to how privacy is understood today.

35 Roger Clarke, 'What's Privacy?', (Workshop at the Australian Law Reform Commission, July 2006) <http://www.rogerclarke.com/DV/Privacy.html>.

36 Roger Clarke, 'A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy' (2016) *Datenschutz Datensich*, pgs 79-83 <https://link.springer.com/article/10.1007/s11623-016-0550-9>.

37 Anita L Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press 2011) pgs 6-11 and 25-26.

38 Koops, Newell, Timan, Škorvánek, Chokrevski, and Galič, 'A Typology of Privacy' (2017, *University of Pennsylvania Journal of International Law*, pg. 483) <https://scholarship.law.upenn.edu/jil/vol38/iss2/4>.

1.4 Evolution of data protection principles

Contemporary conceptions of the right to privacy have carved out informational privacy as a distinct category. This has been a direct response to rapid technological advancements and the associated need to secure the digital lives of citizens, including their personal information. As both private and state actors increasingly rely on the gathering and processing of data to ensure the delivery of products and services, enacting data protection laws has emerged as the foremost step in protecting the informational privacy of individuals. This section discusses the evolution of data protection principles as an important element of the right to privacy and evolving global commitments.

The definition of privacy as control over personal information influenced the development of the Fair Information Practice Principles (FIPPS) in the 1970s.³⁹ These specialised principles and guidelines constitute the foundation from which modern data protection laws have evolved.



39 Austin, Lisa M., 'Re-reading Westin' (2019) 20 *Theoretical Inquiries in Law* 1, pgs. 53-81 <https://din-online.info/pdf/th20-1-5.pdf>

1.4.1 Origin of Fair Information Practice Principles (FIPPS)

The 1970s witnessed intense investigations and legislative deliberations about privacy and data protection across the globe. For instance, the US Congress passed the Privacy Act 1974 after vigorous deliberations in the wake of the Watergate scandal. The Act established the US Privacy Protection Study Commission to further evaluate, research and make recommendations to protect privacy.⁴⁰ Similarly, European countries like Sweden, Germany and France also enacted privacy laws in the 1970s.⁴¹

The FIPPs, which first emerged in the US, are internationally recognised guidelines about the protection of individuals' informational privacy. Most modern data protection laws and guidelines are based on them. They are often described as a minimum set of principles that an effective data protection law should incorporate.⁴² The FIPPS have been included in the data protection laws of over 100 countries⁴³ and in international guidelines and frameworks, such as the UN Guidelines for the Regulation of Computerized Personal Data Files (1990), the EU Data Protection Directive (1995), and the APEC Privacy Framework of the Asia-Pacific Economic Cooperation (2015).

The FIPPs were first articulated in a report by the US Department of Health, Education and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems titled *Records, Computers and the Rights of Citizens* in 1973.⁴⁴ The report recommended the enactment of laws to enforce the Code of First Information Principles articulated in its report. Many of these recommendations were incorporated in the U.S. Privacy Act 1974, which established principles of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals by federal agencies, which include:

- Personal data record keeping systems should follow a “policy of openness” and should not be ‘secret’;
- Records should be accessible and rectifiable by an individual about whom the data is stored;
- The use of personal data should be limited by the purpose of its collection;
- the record-keeping organisation should ensure that “reasonable and proper information management policies” are followed, and information about an individual is necessary, lawful accurate and current.

40 Office of Privacy and Civil Liberties, 'Overview of The Privacy Act of 1974' (United States Department of Justice, 2020) <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>.

41 Robert Gellman, 'Fair Information Practices: A Basic History' (Independent, 3 Sept 2021) <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf>

42 Graham Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance And Global Trajectories' (2014) *Journal of Law, Information and Science*, <http://www.austlii.edu.au/au/journals/JLInfoSci/2014/2.html>

43 Robert Gellman, 'Fair Information Practices: A Basic History' (Independent, 3 September 2021) <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

44 Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 'Records Computers and the Rights of Citizens' (Library of Department of Justice, July 1973) <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

1.5 Introduction to the Identified Regional Frameworks

The FIPPs also form the core of several important and leading regional data protection frameworks, discussed below. These frameworks reflect both the regional diversity in, and universality of, data protection efforts, with frameworks from the Americas, Africa, the Asia-Pacific region, the Caribbean, and Europe. Certain frameworks transcend specific regions and are the product of inter-governmental organisations with cross-cutting memberships from different regions, and include countries from both the Global South and the Global North.

The regional frameworks reflect each region or organisation's consensus on the regulation of and best practices for data protection. A summary of these frameworks demonstrates that there are several common threads tying them together. For instance, they all espouse fundamental data protection principles such as notice and consent, transparency and accountability, security safeguards, purpose limitation, rights of data subjects, and a complaints mechanism. Nevertheless, there are crucial differences in how each framework approaches and applies these principles based on the regional diversity that the frameworks represent. Consequently, a study of the regional frameworks is necessary for a truly holistic understanding of data protection regimes around the world. The following paragraphs briefly outline the Identified Regional Frameworks that will be examined in this report.

1.5.1 OECD Guidelines

In the 1970s, several Member States of the Organisation for Economic Cooperation and Development (OECD) enacted data protection laws based on the FIPPs. To prevent disparities in national legislations that could hamper the free flow of personal data across frontiers and cause disruption to different economic sectors, the OECD developed guidelines to harmonise national data protection

legislation, with the twin aims of upholding human rights and preventing disruptions in international data flows.

The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)⁴⁵ are among the most widely accepted and influential operationalisations of the FIPPs. They are not legally binding and only provide recommendations for minimum data protection standards. When the Guidelines were adopted in 1980, only about one third of the Member States had adopted a data privacy law. By 2011, almost every OECD Member State had a data privacy law with the FIPPs at its core. The 1980 Guidelines were revised in 2013, but the essence of the principles was retained. The Guidelines were revised in tandem with the “changing technologies, markets and user behaviour, and the growing importance of digital identities.”⁴⁶ Two main themes govern the updated Guidelines. First, a focus on the practical implementation of privacy protection through an approach grounded in risk management. Second, the need for greater efforts to address the global dimension of privacy through improved interoperability. The 2013 Guidelines have been published alongside the 1980 Guidelines and a supplementary report to form a comprehensive OECD Privacy Framework (OECD Guidelines).

Therefore, the OECD Guidelines continue to serve the twin goals of preserving privacy and ensuring the free flow of data, while staying relevant in the fast-evolving digital landscape. These Guidelines represent a consensus on the basic principles of data protection which have been built into several national legislative frameworks and are likely to be a guiding force for many other countries that are yet to adopt a data protection law. The OECD Guidelines are not directly binding on OECD members, which continue to enact national data protection statutes. But the Guidelines and associated commentary focus on the formulation

45 OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data' (Sept 1980), <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.

46 'The OECD Privacy Framework' (2013), www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

of basic personal data protection principles which can be built into domestic data protection legislation. The OECD Guidelines consider the regulatory culture of the Member States and allow for context-specific adoption of the Guidelines in each state, which has ensured their continued and widespread relevance.

1.5.2 Convention 108 and 108+ (Council of Europe)

In 1981, the Council of Europe (CoE) adopted its first legally binding international instrument on data protection.⁴⁷ The Convention on the Protection of Individuals with Regards to Automated Processing of Personal Data (Convention 108) is similar to the OECD Guidelines in its twin aims of safeguarding informational privacy and ensuring the trans-frontier flow of personal data. It has been ratified by all 46 Member States of the CoE and by nine non-CoE countries.⁴⁸ Convention 108 embodies the FIPPs and addresses the quality of data, special categories of data, data security, and individual rights to access, correction, and erasure. Convention 108 consists of three key parts: (i) basic principles of data protection; (ii) rules on transborder data flows; and (iii) guarantees of cooperation and mutual assistance between Member States. It was also the first instrument to introduce the concept of adequacy for the exchange of data between two countries. In 2018, Convention 108 was modernised through an amending protocol to address the challenges of rapidly advancing technology and growing data processing volumes. The resulting instrument, described as Convention 108+, introduced the need for regulatory authorities, the principles of proportionality and data minimisation, and addressed issues of algorithmic decision making. Convention 108+ has been signed by 43 Member States.⁴⁹ It was clarified that “the principles of transparency, proportionality, accountability, data minimisation, privacy by design, etc. are now acknowledged as key elements of the protection mechanism and have

been integrated in the modernised instrument”.⁵⁰ The instrument requires Member States to apply the principles set out in the convention to their domestic legislation.

1.5.3 Data Protection Directive, 1995 and GDPR (European Union)

One of the most important regional frameworks governing data protection is the EU’s General Data Protection Regulation (GDPR), which came into force in 2018, replacing the Data Protection Directive. The Data Protection Directive was one of the first regional instruments on data protection and “contained one of the world’s most stringent implementation of the FIPPs.”⁵¹ It laid down a framework for data protection for all EU Member States and required them to enact implementing national legislation. However, the Data Protection Directive failed to fully harmonise national data protection laws within the EU, and this resulted in enforcement problems. For example, the Data Protection Directive allowed EU Member States flexibility in setting fine amounts for violations of the Directive, and some EU Member States set their maximum fines under the Directive to very low amounts, which has made the sanction process, in the opinion of some commentators, ineffective.⁵²

The GDPR was enacted to meet the EU’s need for a comprehensive approach to data protection. The GDPR imposes binding obligations, and is applicable not only on Member States, but also to organisations outside EU territory if they target or collect data related to data subjects in the EU. The extra-territorial application, and binding nature of the GDPR, are some of the most distinctive features of this instrument.

47 Council of Europe, 'Convention for the Protection of Individuals with Regards to the Automatic Processing of Individual Data', (ETS 108, Jan 1981), <https://www.refworld.org/docid/3dde1005a.html>.

48 Council of Europe, 'Chart of Signatures and Ratifications of Treaty 108', <https://www.coe.int/en/web/conventions/full-list>.

49 Council of Europe, 'Chart of Signatures and Ratifications of Treaty 223', <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyid=223>.

50 Council of Europe, 'Modernisation of Convention 108' (2018), <https://www.coe.int/en/web/data-protection/convention108/modernised>.

51 Borgesius, Gray and Van Eechoud, 'Open Data, Privacy, and Fair Information Principles: Towards A Balancing Framework', (2015), *Berkeley Technology Law Journal*, <https://lawcat.berkeley.edu/record/1127406>.

52 Hoofnagle, van der Sloot and Borgesius, 'The European Union General Data Protection Regulation: What It Is And What It Means' [2019] *Information and Communications Technology Law*, <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501>.

1.5.4 Commonwealth Framework (Commonwealth of Nations)

There is no binding framework that is applicable to all Commonwealth countries. The Commonwealth frameworks for data protection recognise diversity and seek to promote the 'best fit' instead of best practice.⁵³ In 2002, the Commonwealth Law Ministers released three inter-related model Bills on privacy and freedom of information, namely the Freedom of Information Bill, the Privacy Bill, and the Protection of Personal Information Bill. These model bills seek to assist Commonwealth nations which are yet to enact laws regulating the access to, processing and protection of personal information by providing them with a model framework to serve as a useful starting point for draft legislation. The Privacy Bill and the Protection of Personal Information Bill deal with the regulation of informational privacy.

The Protection of Personal Information Commonwealth (PPI Bill) focuses on the processing of personal information by private organisations and acts as a model data protection bill for countries seeking to enact such legislation. It does not apply to public authorities or to information processed for personal or domestic, journalistic, artistic, or literary purposes. The Commonwealth Privacy Bill was created to give effect to the OECD guidelines and regulates data processing by public authorities.⁵⁴

1.5.5 APEC Privacy Framework (Asia-Pacific Economic Cooperation)

The APEC Privacy Framework was published in 2004 and updated in 2015. It seeks to set a common data privacy standard for the 21 APEC member economies in the Asia-Pacific region. The framework aims to protect data privacy while facilitating the free flow of

cross-border data in the APEC region.⁵⁵ The APEC's principle-based framework seeks to move towards common standards resulting in consistent – rather than identical – privacy protections in the region. The framework aims to reconcile the need for consumer privacy with business and commercial interests, while recognising the cultural and other diversities that exist within the member economies. The APEC Privacy Framework does not impose binding obligations on member economies that undertake the commitments on a voluntary basis.

In addition to the privacy frameworks, the region also has the APEC Cross-Border Privacy Rules (CBPR System). The CBPR System is a government-backed data privacy certification that companies can adopt to demonstrate compliance with internationally recognised data privacy protections. The CBPR system is used to implement the principles recognised by the APEC Privacy Framework.⁵⁶

1.5.6 HIPCAR - Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean Community (Caribbean Community)⁵⁷

The HIPCAR project was launched by the International Telecommunications Union and the European Union in Grenada in December 2008, in collaboration with the Caribbean Community Secretariat and the Caribbean Telecommunications Union.⁵⁸ Its objective was to harmonise ICT laws and policies in the Caribbean region by working with Caribbean governments, regulators, service providers, and civil society. The HIPCAR framework provides for six inter-related model frameworks on subjects ranging from eCommerce, Interception of Communications and Cybersecurity. One of these frameworks, the HIPCAR Model Policy Guidelines on Privacy and Data Protection, suggest that Member States adopt

53 'Data Protection in the Commonwealth - Key Instruments Current Practices' (The Commonwealth, 20 April 2016), https://unctad.org/system/files/non-official-document/dtl_eweek2016_EBakibinga-Gaswaga_en.pdf.

54 The Commonwealth (Office of Civil and Criminal Justice Reform), Model Privacy Bill, https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_9_ROL_Model_Privacy_Bill_0.pdf.

55 APEC Privacy Framework, part i, preamble

56 APEC Secretariat, 'What is the Cross-Border Privacy Rules System?' (15 April 2019) <<https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system>

57 The Caribbean Community (CARICOM) is a group of twenty countries (twenty members and five associate members) including Grenada, Barbados, Saint Lucia, Jamaica, and Montserrat. CARICOM countries are home to an estimated 16 million people. See CARICOM, Who we are <<https://caricom.org/our-community/who-we-are>

58 Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts' (HIPCAR, 2012) <<https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf>

a clear legal and institutional framework ensuring the protection of personal information, adherence to key data protection principles and appropriate governance structures. While the Model Policy Guidelines are not legally binding on Member States, the framework constitutes a valuable resource for national authorities seeking to develop domestic data protection legislation.

1.5.7 The African Union Convention (African Union)

The African Union Convention on Cyber-Security and Personal Data Protection (AU Convention) was adopted by the AU in 2014. The AU Convention is different from other regional frameworks examined, in that it aims to facilitate regional and national legal frameworks for cybersecurity, prevention of cyber-crime and electronic transactions, in addition to personal data protection. The AU Convention attempts to strengthen existing ICT legislation within the African Union⁵⁹, making it a valuable resource for countries seeking to develop domestic data protection legislation. It highlights the necessity of adhering to national constitutions and regional and international human rights law when creating and implementing data protection laws.⁶⁰

1.5.8 Organization of American States Principles

The Organization of American States (OAS) released the Preliminary Principles and Recommendations on Data Protection in 2011.⁶¹ The OAS's Inter-American Juridical Committee released the OAS Principles on Privacy and Data Protection in 2015.⁶² In November 2021, the General Body of the OAS adopted the Updated Principles on Privacy and Personal Data

OAS Principles,⁶³ which serve as a guide for national frameworks in the region. The OAS Principles are accompanied with annotations by the Juridical Committee that provide valuable context and additional detail to each principle.

The OAS Principles contain 13 principles, which serve as a basis for data protection legislation. The principles are not binding, but rather they generally focus on the goals to be achieved by national legislation. The principles are meant to act as general guidelines which the Member States may choose to follow when developing their domestic legislation.

1.5.9 ASEAN Frameworks (ASEAN region)

The Association of South-East Asian Nations (ASEAN) region has two main data protection frameworks, namely the ASEAN Framework on Personal Data Protection, introduced in 2016,⁶⁴ and the ASEAN Framework on Digital Governance (ASEAN Digital Governance Framework), introduced in 2017.⁶⁵ Both instruments seek to foster regional integration and cooperation and promote the growth of trade and flow of information within and among ASEAN Member States and boost their digital economies. The framework's provisions are not binding. Instead, they highlight the consensus amongst ASEAN members on the importance of harmonised and robust national data protection laws and set out certain principles that such laws should be guided by.

59 African Union Convention on Cyber Security and Personal Data Protection, Preamble https://www.opennetafrica.org/?wpfb_dl=4

60 NATO Cooperative Cyber Defence Centre of Excellence, 'Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection' (2015) <<https://ccdcoe.org/incyber-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/>

61 Department of International Law, of the Secretariat for Legal Affairs, 'Preliminary Principles and Recommendations on Data Protection' (Committee on Juridical and Political Affairs-OAS, Oct 2011), http://www.oas.org/dil/CP-CAJP-2921-10_rev1_corr1_eng.pdf.

62 86th Regular Session, 'Protection of personal data - Organization of American States' (OAS, Mar 2015), https://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf.

63 Inter-American Juridical Committee, Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with Annotations, http://www.oas.org/en/sla/iajc/docs/CJI-doc_638-21_EN.pdf.

64 ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Framework on Personal Data Protection, Nov 2016, https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.

65 ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Framework on Digital Data Governance, Dec 2018, https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.

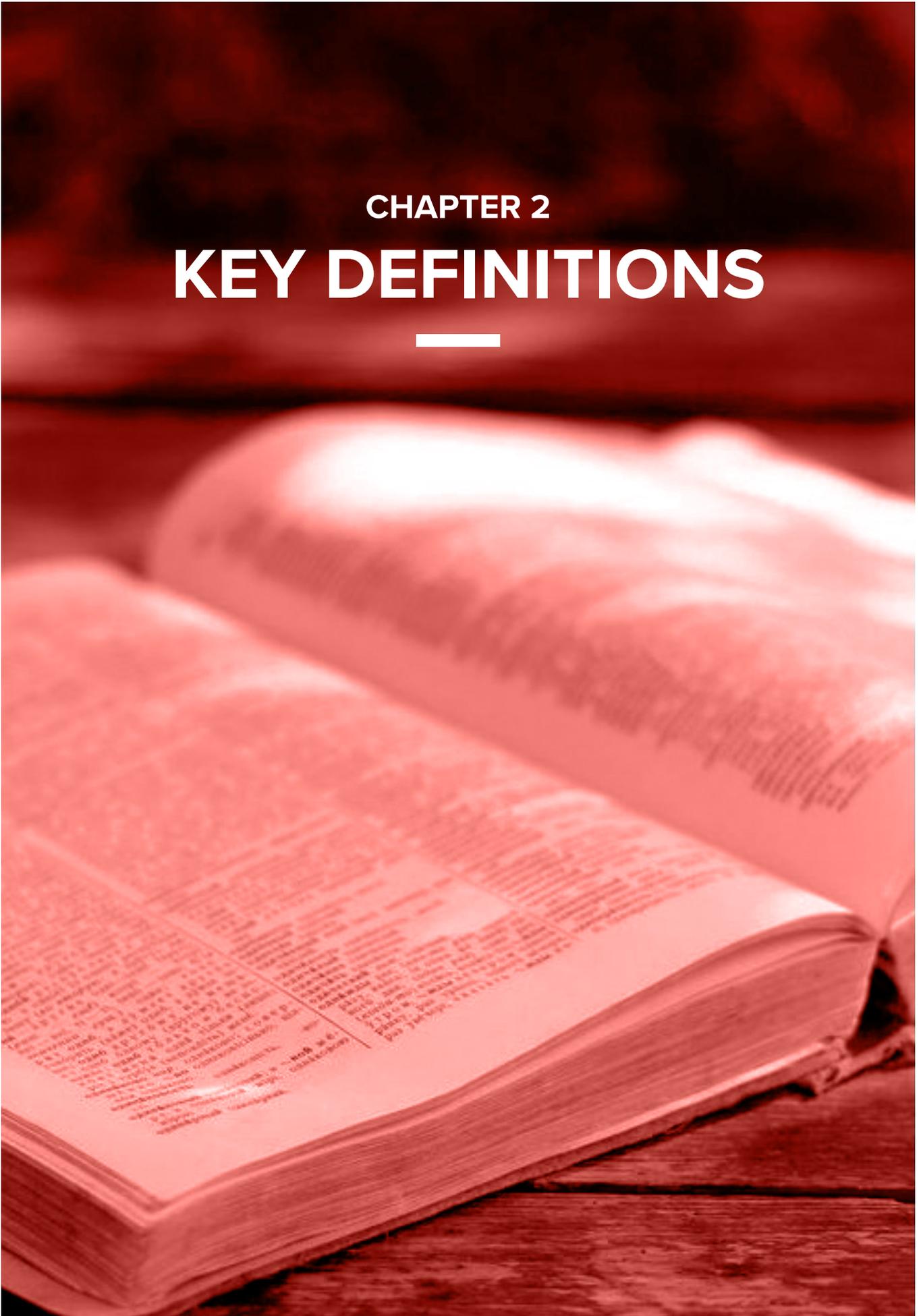
1.6 Conclusion

Legal identity programmes have emerged as crucial tools for: the securing of sustainable development goals; the formulation, implementation, and monitoring of public policy; and the eradication of systemic discrimination. However, legal identity programmes raise a corollary concern for the right to privacy of the individuals whose data is being collected and processed in the operationalisation of these programmes. The adoption of the Identified Regional Frameworks demonstrates a widespread recognition of the need and desire to protect the privacy of individuals as legal identity programmes are implemented across the world. Data protection has emerged as a key tool to guarantee the right to privacy, autonomy, and dignity of the individual without stymieing legal identity programmes or technological innovation. The remaining chapters of this report discuss the various elements of data protection legislation based on a study of the Identified Regional Frameworks.



CHAPTER 2

KEY DEFINITIONS



2.1 Introduction

This chapter highlights some frequently used terms in the data protection and privacy sphere across the Identified Regional Frameworks, and discusses the challenges associated with each term. In data protection law, a chapter on definitions is usually necessary and serves three basic functions: (i) it permits conciseness by conveying key concepts in one or two words; (ii) it helps reduce the risk of ambiguity in interpretation of these concepts; and (iii) it defines the scope of applicability of the framework. All the Identified Regional Frameworks include a set of definitions, except for ASEAN's frameworks on Personal Data Protection and Digital Governance.

2.2 Personal Data and Personal Information

The definition of personal data is a key determinant in deciding the scope of a data protection framework. Upon defining personal data or information, the data or information covered by the definition is regulated by the data protection framework. Any data or information not covered by the definition falls outside the framework's protections. All Identified Regional Frameworks that have a definitions clause, provide a definition of either the term 'personal data' or 'personal information'. The concept of personal data is centred around the idea of the identifiability of an individual. It is generally understood that 'personal data' is a broader term than 'personal information.' This is because all the elements of personal information, or personally identifiable information (PII), are subsumed within the concept of personal data.

The OAS Principles specifically highlight the difference between data and information. They note that the term personal data is used intentionally because it provides the "broadest protection to the rights of the individuals concerned without regard to the particular form in which the data is collected, stored, retrieved, used or disseminated."⁶⁶ They clarify that the term 'personal information' has been avoided as it could be construed literally and might not "include

specific data", such as factual items or electronically-stored "bits" or digital records". Scholars have also expressed preference for the term personal data and have argued that it allows for "the inclusion of data used by future technologies and new methods of doing business."⁶⁷ In the case when a framework defines personal data in a broad and open-ended manner, it allows the framework to adapt to many contexts and to be interpreted widely by the courts and authorities.

The GDPR defines the term personal data to include information relating to an identified or identifiable natural person.⁶⁸ It further provides for the definition of an identifiable natural person as one "who can be directly or indirectly identified" in reference to a list of identifiers and a range of factors. A non-exhaustive list of identifiers is set out including name, identification number, location data, and an online identifier. The range of factors include physical, physiological, genetic, mental, economic, cultural or social identity of a natural person. It provides that an individual can be identified directly or indirectly through one of the identifiers, or a combination of identifiers and factors specified above.

66 OAS Principles with Annotations, Definitions, (Page6 definition of personal data).

67 Voss WG and Houser KA, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies' (2019) 56 American Business Law Journal 287.

68 GDPR, art 4(1).

“Personal data being a broad and open-ended term allows for it to be interpreted widely in favour of data subjects and help secure their fundamental rights.”

The influence of the GDPR is widely acknowledged. Many countries have gravitated towards it when framing their data protection frameworks. However, a study of the Identified Regional Frameworks reveals that several regional frameworks have adopted a similar definition of personal data irrespective of whether adopted before or after the GDPR and include the AU Convention, the Convention 108+, the OAS Principles, the OECD Guidelines and the APEC Privacy Framework. For example, the 2014 AU Convention also defines personal data as data that directly or indirectly identifies an individual.⁶⁹ The OAS Principles substitute the term identifiable individual with information that “reasonably” identifies a specific individual directly or indirectly.⁷⁰ Convention 108+ also introduces the element of reasonableness by stating that data does not identify an individual if their identification requires “unreasonable time, effort or resources.”⁷¹

Several of the Identified Regional Frameworks provide an illustrative list of identifiers or factors that would render an individual identifiable, and could consequently cause the data to be treated as personal data.⁷² Other frameworks do not provide a list of factors or identifiers,⁷³ however, relying, instead on the concept of identifiability. For example, the Explanatory Report to Convention 108+, when discussing the notion of an identifiable individual, refers to aspects or traits that individualise or single out one person from others, which allows scope for differential treatment.⁷⁴ It does not refer to any specific aspect or traits.

69 Art 1 (definition of personal data).

70 OAS Principles with Annotations, Definitions, page 6 (definition of personal data).

71 Explanatory Report to Convention 108+, para 17 p. 17.

72 Commonwealth PPI Bill, S 4; Commonwealth Privacy Bill S 4; HIPCAR Model Legislative Text, S 3(1)(h). Identifiers and factors in the HIPCAR Privacy Framework include nationality, address, age, marital status, racial or ethnic origins, education, and employment and educational records. The Commonwealth PPI Bill and Privacy Bill use similar identifiers including identifying numbers and medical and criminal records.

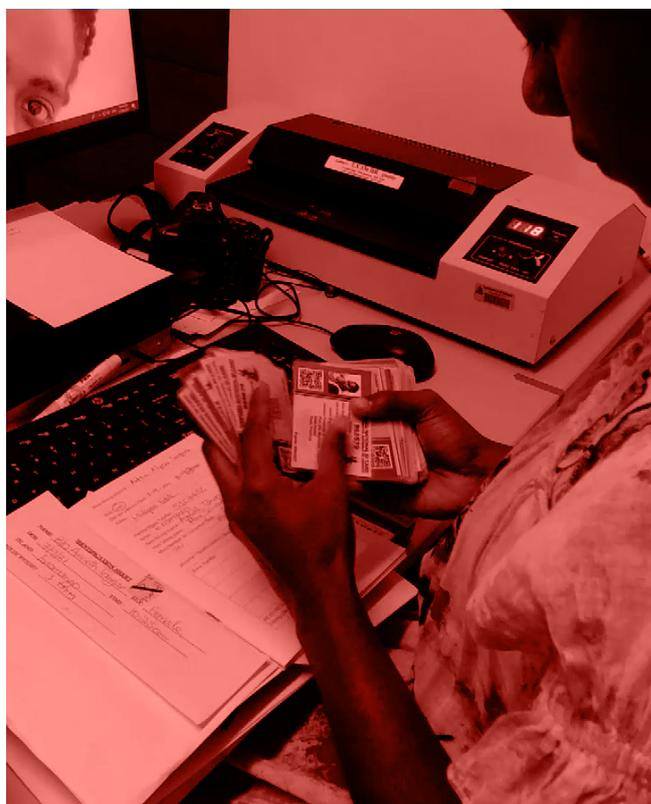
73 See Convention 108+; OECD Guidelines; APEC Privacy Framework.

74 Explanatory Report to Convention 108+, para 18 p.17.

A framework adopting a broad definition of personal data would result in more data being regulated by the data protection framework. For some time now, researchers have been deliberating about the scope of ‘personal data’, with some even expressing criticism that the expanding definition of personal data has become too broad.⁷⁵ Understandably, a wide definition of personal data would provide the highest legal protection, but it may, in practice, be challenging to ensure compliance, and may, as a consequence, be deemed unreasonable. For instance, the GDPR offers a broad definition of the term personal data and focuses on whether the available data can identify a natural person based on “an analysis of all means likely to be used and by reference to available data.”⁷⁶ The benefit of this broad definition is that almost nothing is outside the scope of EU privacy regulation. The drawback is that information is treated as personal data, and uniformly high compliance burdens are created, irrespective of whether the data refers to an identified individual, or one who can be “indirectly identified” – i.e., someone who is “identifiable.” This has prompted discussions on the need to create a definition of personal data based on the risk of identification, whereby data protection is triggered by the probability that the data identifies an individual.⁷⁷ The concept is especially relevant when data may be anonymised or pseudonymised to reduce the risk of identification.

However, a wide definition of personal data need not necessarily give rise to onerous compliance burdens or implementation challenges if the provisions operationalising data protection principles are applied strategically and are based on identifiability. The obligations related to notification and consent, for example, may be exempted in situations where the data being processed does not directly identify individuals. Such a targeted and nuanced approach helps preserve the benefit of adopting a broad definition of personal data. Personal data being a broad and open-ended term allows for it to be interpreted widely in favour of data subjects and help

secure their fundamental rights. For example, the ECJ interpreted the definition of personal data to include, names and addresses, names with a telephone number, dynamic IP address, biometric data, and individuals’ video images.⁷⁸



75 Purtova N, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10 *Law, Innovation and Technology* 40.

76 Schwartz PM and Solove DJ, ‘Reconciling Personal Information in the United States and European Union’ (2014) 102 *California Law Review* 877, 887.

77 Purtova N, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10 *Law, Innovation and Technology* 40; Schwartz PM and Solove DJ, ‘The PII Problem: Privacy and a New Concept of Personally Identifiable Information’ (2011) 86 *New York University Law Review* 1814.

78 Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 1–2 (Oct. 19, 2016) <http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0582&lang1=fr&type=TEXT&ancre=>.

2.3 De-identification Methods

Emerging scholarship about de-identification and personal data protection acknowledges that data identifiability cannot be seen as binary, whereby personal data is covered under data protection frameworks and anonymised data is not.⁷⁹ Discussions have progressed from the dichotomy of whether data is personally identifiable or not to a trichotomy, which comprises of identified, identifiable (possible risk of identification) and non-identifiable (remote risk of identification). This allows for shades of de-identified data to be recognised within the category of personal information, based on the probability or risk that such de-identified data may ultimately lead to individuals being identified.

Data has multiple gradients of identifiability, and the process of de-identification helps remove information that may identify individuals from existing personal data. Depending on the purpose of processing, different types of de-identification methods may be used. De-identification has a wide spectrum, whereby different levels of de-identification have different regulatory and policy implications. For instance, anonymised data is generally kept outside the purview of data protection frameworks, and softer and fewer obligations apply to pseudonymised data in comparison to identifiable and identified data.

Although the need and value of de-identification tools is widely acknowledged and reflected in many new and emerging frameworks, there exists a lack of uniformity in adopting standards of de-identification and common terminology.⁸⁰ Frameworks may not

refer to de-identified data or de-identification, and may instead use de-identification techniques, such as anonymisation and pseudonymisation. Some recent data protection frameworks, such as the GDPR, recognise intermediate de-identification tools by introducing the concept of pseudonymisation/pseudonymised data, and also the highest form of de-identification, i.e., anonymised data, with the latter explicitly kept outside the purview of the framework.⁸¹ However, legislation drafted post GDPR, such as India's Data Protection Bill and China's Personal Information Protection Law, merely recognise anonymised data.⁸²

To steer clear of the definitional ambiguity, and to better understand the terminologies and taxonomy of de-identified data, we discuss the three most widely used terminologies below, which are anonymised data, pseudonymised data, and de-identified data.

2.3.1 Anonymised Data

The term "anonymisation" can be described as a process that breaks the identifiability link between identifying data and an individual. Privacy laws across the globe indicate that 'anonymised' data is not subject to principles of data protection since it does not contain any PII, eliminating any attributes that will directly or indirectly identify the individual. For example, anonymised data under the GDPR can be shared freely and does not come within the Regulation's ambit.⁸³

79 Mike Hintze, 'Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance' (Future of Privacy Forum, 2016), <https://fpf.org/wp-content/uploads/2016/11/M-Hintze-GDPR-Through-the-De-Identification-Lens-31-Oct-2016-002.pdf>.

80 Polonetsky J, Tene O and Finch K, 'Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification' (2016) 56 Santa Clara Law Review 593.

81 GDPR, recital 26.

82 Personal Information Protection Law, China 2020), 2. 73(4) (China) <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>; Data Protection Bill (2021) S. 3(2) (India) http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf. India's pending data protection legislation was first introduced into Parliament as the 'Personal Data Protection Bill, 2019' and referred to a Joint Parliamentary Committee for additional scrutiny. The revised bill, as reported by the Joint Parliamentary Committee, is titled the 'Data Protection Bill, 2021'.

83 GDPR, recital 26.

The OAS Principles expressly define the term anonymization as “measures of any nature aimed at preventing the identification or reidentification of natural persons without disproportionate effort.”⁸⁴ The term is discussed in recitals to the GDPR,⁸⁵ while the Explanatory Report to Convention 108+ notes that data is only to be considered anonymous if it is either impossible to re-identify individuals, or such re-identification would require unreasonable effort or resources.⁸⁶

The following are the essential characteristics of anonymised data:

2.3.1.1 Not identifiable

The GDPR’s Recital 26 states that information that does not relate to an identified or identifiable person is ‘anonymous information’. Both direct and indirect identifiers should be removed, transformed, or distorted to an extent which guarantees that data cannot be linked to an individual.

2.3.1.2 Avoids re-identification

As stated, PII must be “irreversibly” removed for data to be considered anonymous. However, it has been suggested that since irreversible anonymisation is often not possible, it is best to assess the degree of risk associated with re-identification.⁸⁷ The GDPR considers data to be anonymous if it is not “reasonably likely” to identify the concerned data subject,⁸⁸ while Convention 108+ notes that anonymous information must either be impossible to re-identify or require an “unreasonable level of effort or resource” to re-identify.⁸⁹

Some studies show that anonymised data can be re-identified⁹⁰ particularly as a result of technical innovations. Re-identification is primarily carried out by linking large publicly available datasets and other auxiliary data or metadata to the anonymised data. Therefore, when assessing the risk of re-identification, factors such as the time and cost of potential re-identification, and technological advancements, should be considered. Increasing the threshold against re-identification ensures that potential personal data does not elude the intended scope of data protection frameworks. Additionally, legislation can provide appropriate redress and compensation to those harmed by wrongful re-identification.

2.3.1.3 Application of data protection principles

Generally, because anonymised data is not personal data, it does not come under the scope of regulations governing data privacy.⁹¹ However, it has been argued that because there always exists a risk of re-identification with anonymised data, certain standards of data protection principles must continue to be applied to anonymised data as well.⁹² The French National Administrative Court has noted, for example, that data can only be anonymous if any direct or indirect identification is impossible.⁹³ The ECJ has also ruled that data allowing indirect identification of individuals must be considered personal data.⁹⁴ This is because metadata consisting of time and place of communication combined with other data, such as IP address assist with re-identification.

84 OAS Principles with Annotations, Definitions, page 6.

85 GDPR, recital 26. “The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”

86 Explanatory Report to Convention 108+, Paras 19 and 20 p. 17.

87 Alvaro Moreton, ‘The problem of complete, irreversible anonymisation’, (Comprise, 28 December 2020) <https://www.compriseh2020.eu/the-problem-of-complete-irreversible-anonymisation/>.

88 GDPR, recital 26.

89 Explanatory Report to Convention 108+, paras 19 and 20.

90 Lubarsky B, ‘Re-Identification of “Anonymised Data” (2017) 1 Georgetown Law Technology Review 202.

91 Ian Walden, ‘Anonymising Personal Data’ (2002) 10 Int’l J.L. & Info. Tech., 224.

92 Michèle Finck, Frank Pallas, ‘They who must not be identified—distinguishing personal from non-personal data under the GDPR’ (2020) 10 1, International Data Privacy Law, 11-36.

93 Conseil d’État, 10ème – 9ème ch. réunies, décision du 8 février 2017, N° 393714 (citing art 2 of the Law of 6 January 1978); Michèle Finck, Frank Pallas, ‘They who must not be identified—distinguishing personal from non-personal data under the GDPR’ (2020) 10 1, International Data Privacy Law, 11-36.

94 Cases C-293/12 And C-594/12, [2014] Eu:C:2014:238; Michèle Finck, Frank Pallas, ‘They who must not be identified—distinguishing personal from non-personal data under the GDPR’ (2020) 10 1, International Data Privacy Law, 11-36.

To mitigate the privacy risks, experts have suggested that anonymised data should remain within the definition of personal information, but only a selective application of data protection principles be carried out.⁹⁵

2.3.2 Pseudonymised Data

Like anonymisation, pseudonymisation is also a security measure adopted by data controllers and supports the data minimisation principle.⁹⁶ Pseudonymisation differs from anonymisation by being a reversal process; whereby pseudonymised data can be combined with additional information to enable re-identification.⁹⁷ In contrast, once data is anonymised, re-identification should be impossible or require unreasonable effort. Data controllers can choose either anonymisation or pseudonymisation based on the type of data that is being processed, the purpose of data processing, and the risk of a data breach.

The process of pseudonymisation “consists of replacing one attribute (typically a unique attribute) in a record by another” and is not a method of anonymisation.⁹⁸ By employing pseudonymisation, the identity of the data subject is substituted with a pseudonym, which does not disclose an individual’s personal information. The pseudonym is an additional piece of information accessible only by the pseudonymising entity. It is merely a substitute and can be reversed. The re-identification would depend on additional information, such as a reference number. For example, the Internet company AOL released pseudonymised search data of its users in 2006, replacing users’ names with numbers; but a simple investigation of users’ search results led to the re-identification of several users, including their real names and locations.⁹⁹

Pseudonymisation is considered a useful security



95 Smitha Krishna Prasad, Yesha Paul and Aditya Singh Chawla, ‘Comments on the Draft Personal Data Protection Bill, 2018’ (2018) Centre for Communication Governance at NLU Delhi, p. 29 <https://www.medianama.com/wp-content/uploads/CCG-NLU-Submission-India-Draft-Data-Protection-Bill-Privacy-2018-and-Srikrishna-Committee.pdf>.

96 Gerald Spindler, Philipp Schmechel, ‘Personal Data and Encryption in the European General Data Protection Regulation’ (2016) 7, JIPITEC 163.

97 Information Commissioner’s Office, Introduction to Anonymisation, (Draft Anonymisation, Pseudonymisation, And Privacy Enhancing Technologies Guidelines, May 2021), p 4 <https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>.

98 European Commission, EUROPA, Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, (10 April 2014) 3 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

99 Michael Barbaro and Tom Zeller Jr., ‘A Face Is Exposed for AOL Searcher No. 4417749’ (New York Times, 09 August 2006) <https://www.nytimes.com/2006/08/09/technology/09aol.html>.

measure since it reduces the risk of link-ability of a dataset with the identity of the data subject.¹⁰⁰ Companies can use it to enable secondary use of data, such as service evaluation or research. In addition, whether data is pseudonymised may be one of the factors to assess in determining whether additional processing of data beyond the original purpose should be permitted; for example, for scientific, historical or statistical purposes.¹⁰¹

Of the Identified Regional Frameworks, only the GDPR and the Convention 108+ regulate the use of pseudonymised information. Both these frameworks consider pseudonymised data as personal data, and subject it to the principles of data protection.¹⁰² As per Convention 108+, the quality of the pseudonymisation technique must be assessed on the basis of privacy safeguards incorporated in the technique.¹⁰³

2.3.3 De-identified Data

De-identified data prevents re-identification by removing or manipulating both direct and known indirect personal identifiers. Like anonymisation and pseudonymisation, it is also a useful data minimisation technique executed by data controllers to protect the privacy rights of individuals and re-use data or share it with third parties.¹⁰⁴ De-identified data is often used for medical and pharma-related research. For instance, sensitive health data can be de-identified by removing identifiers that would allow individual patients to be discerned and used to analyse market trends and efficacy of a drug.

Of the frameworks studied, only the Commonwealth PPI Bill specifically provides for the definition of ‘de-identify.’¹⁰⁵ Section 4 of the Bill defines de-identification as the removal of information which: (i) identifies the individual; (ii) can be manipulated by a foreseeable method to identify the individual; and (iii) can be linked by a foreseeable method to other information which identifies the individual or can be foreseeably manipulated to identify an individual.

“Data has multiple gradients of identifiability, and the process of de-identification helps remove information that may identify individuals from existing personal data. Depending on the purpose of processing, different types of de-identification methods may be used.”

100 Waltraut Kotschy, Ludwig Boltzmann, ‘The new General Data Protection Regulation - Is there sufficient pay-off for taking the trouble to anonymize or pseudonymize data?’ Institute for Human Rights, Vienna <https://fpf.org/wp-content/uploads/2016/11/Kotschy-paper-on-pseudonymisation.pdf>.

101 Information Commissioner’s Office, Introduction to Anonymisation, (Draft Anonymisation, Pseudonymisation, And Privacy Enhancing Technologies Guidelines, May 2021), p 4 <https://ico.org.uk/media/about-the-ico/consultations/2619862/Anonymisation-Intro-And-First-Chapter.Pdf>.

102 GDPR, recital 26; Convention 108+, Explanatory Report, para 18.

103 Convention 108+, Explanatory Report, para 18-20.

104 Khaled El Emam, Guide to De-Identification of Personal Health Information (CRC Press 2013) 135.

105 Commonwealth PPI Bill, s 4 (definition of “de-identify”).

2.4 Data subject

The definition of data subject is considered “the most important definition” of a data protection framework. Similar to the definition of personal data, it decides the scope of the framework’s application. The term generally refers to a natural person whose personal data undergoes processing, whereby the term ‘processing’ is broadly interpreted to include instances of collection, processing, storage, use, encryption, dissemination, disclosure, and deletion.¹⁰⁶ Any individual whose data is subject to these processes would therefore be a data subject. Data subjects are the primary beneficiaries of data protection frameworks.

A majority of the Identified Regional Frameworks expressly define the term data subjects either in relation to data processing (individuals whose data is being processed),¹⁰⁷ or as individuals identified or identifiable through their personal data (the individual whom the personal data identifies).¹⁰⁸ Some frameworks do not use the term data subject. For example, the Commonwealth PPI Bill and ASEAN DP Framework refer to the beneficiaries whose data is being protected simply as an individual.¹⁰⁹

Most scholars agree that the idea of a data subject relates to a natural living person, and does not include deceased persons.¹¹⁰ However, concerns have been raised with respect to the processing of deceased persons’ data, with certain scholars arguing that the right to privacy could apply to a deceased person as the personality right of the deceased continues to exist.¹¹¹ The Commonwealth PPI Bill extends the scope of its beneficiaries to both living and deceased individuals.¹¹² Although the Explanatory Report to Convention 108+¹¹³ observes that the framework is not intended to cover deceased data subjects, it also provides that individual parties to the Convention may extend protection to deceased persons within their domestic jurisdictions. The HIPCAR Privacy Framework allows for the delegation of a data subject’s rights to the ‘personal representative’ of the deceased data subject.¹¹⁴

106 OAS Principles with Annotations, Definitions, page 6 (Definition of data processor); AU Convention, Article 1 (definition of Processing of Personal Data); Convention 108+, Article 2(b) (definition of data processing); HIPCAR Model Legislative Text, s 3(1)(j) (definition of processing); Commonwealth Model Bill on Personal Information, Section 4 (Definition of “process”).

107 AU Convention, art 1 (Definition of data subject); HIPCAR Model Legislative Text, Section 3(1)(d); OAS Principles with Annotations, Definitions Page 6 (Definition of data subject).

108 GDPR, art 4(1); Convention 108+, art 2(a); OECD Guidelines, Chapter 1, Part 1, para 1(b).

109 Commonwealth PPI Bill, s 4 (definition of individual); ASEAN DP Framework, para 6(a).

110 Edina Harbinja, ‘Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?’ (2013) 10(1) SCRIPTed <https://script-ed.org/article/eu-data-protection-regime-protect-post-mortem-privacy-potential-alternatives/>; GDPR, recital 27 states that the GDPR does not apply to the personal data of deceased persons.

111 Buitelaar JC, ‘Post-Mortem Privacy and Informational Self-Determination’ (2017) 19 Ethics and Information Technology 129.

112 Commonwealth PPI Bill, s 4 (definition of individual).

113 Convention 108+, Explanatory Report, para 30. See also GDPR, recital 27 adopting a similar approach of discretion.

114 HIPCAR Model Legislative Text, s 25.

Data protection frameworks typically protect the personal data of natural persons. The APEC Privacy Framework categorically mentions that the framework is “intended to apply to information about natural persons, not legal persons,” and that personal information relates to information about an identified or identifiable individual.¹¹⁵ However, Convention 108+ allows extending the protection to legal persons to protect their legitimate interests.¹¹⁶

The concepts of personal data and data subject are closely linked. For example, the GDPR defines “data subject” with reference to the definition of “personal data.”¹¹⁷ Article 4(1) GDPR states, “personal data means any information relating to an identified or identifiable natural person (data subject)”. A person becomes a data subject if they “can be identified, directly or indirectly.”¹¹⁸ As with the GDPR, Convention 108+ and the OECD Framework also include a data subject within the definition of personal data.¹¹⁹



115 APEC Privacy Framework, part ii, commentary to para 9

116 Convention 108+, Explanatory Report, para 30.

117 GDPR, art 4(1).

118 GDPR, art 4(1).

119 Convention 108+, art 2(a); OECD Guidelines, Chapter 1, Part 1, para 1(e).

2.5 Specific categories of data

2.5.1 Health data

Healthcare data is increasingly being digitised to generate new scientific insights. The importance of healthcare data has increased exponentially during the COVID-19 pandemic. Data analytics can even help policymakers make more informed healthcare decisions contributing to better public health. There are several examples worldwide where technology platforms are delivering public health services often in partnership with governments to help fight COVID-19.¹²⁰ However, these instances also raise privacy concerns. A recent consumer survey indicated that only 11 percent of people in America were willing to provide technology companies with their health data, as opposed to those willing to provide their health data to pharmaceutical companies (20 percent) or even the government (12 percent).¹²¹

Health data is not limited to data relating to ill health, but also relates to data collected through health and wellness apps.¹²² The WHO acknowledges that health data is a broad umbrella term encompassing eHealth and other emerging sectors, such as the use of advanced computing sciences in big data, artificial intelligence and genomics.¹²³ Against this backdrop, scholars have opined that current regulatory frameworks may be inadequate to regulate current data processing developments in

the health sector.¹²⁴ For instance, the principles of data retention, transparency and consent become difficult to impose and enforce due to the deployment of machine learning techniques, which use large amounts of data that cannot be specifically identified and articulated. Technological developments are therefore expanding the scope of health data that may need to be protected by legal frameworks.

Among the Identified Regional Frameworks, only the AU Convention and the GDPR expressly provide for a definition of the term ‘health data’.¹²⁵ The HIPCAR Privacy Framework, Commonwealth PPI and Privacy Bills cover health-related information within the ambit of their definition of personal information.¹²⁶ Convention 108+ does not expressly define the term but identifies personal data relating to “health or sexual life” as a special category of data requiring additional protection.¹²⁷ Several other frameworks such as the HIPCAR Privacy Framework, and the OAS Principles also mark health data as a sensitive or special category of data.¹²⁸

Health data is generally related to: the past, present, and future, mental or physical state, health, or condition of a data subject.¹²⁹ Health data may include a sick or healthy person, genetic data, or data related to the provision of health care services.¹³⁰

120 Sara Nyman, ‘COVID-19, tech firms, and the case for data sharing’ (World Bank Blogs, 14 July 2020) <https://blogs.worldbank.org/psd/covid-19-tech-firms-and-case-data-sharing>.

121 Christina Farr, ‘Tech companies see health data as a huge opportunity, but people don’t trust them’ (CNBC, 13 February 2019) <https://www.cnn.com/2019/02/13/consumers-dont-trust-tech-companies-with-health-data-rock-health.html>.

122 Article 29 Working Party, ANNEX - health data in apps and devices, 2015; https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

123 Executive Board, mHealth: use of appropriate digital technologies for public health: report by the Director-General, 142. (2017) World Health Organization. <https://apps.who.int/iris/handle/10665/274134>

124 Marelli L, Lievrouw E and Van Hoyweghen I, ‘Fit for Purpose? The GDPR and the Governance of European Digital Health’ (2020) 41 Policy Studies 447.

125 GDPR, art 4(15); AU Convention, art 1 (definition of health data).

126 HIPCAR Model Legislative Text, s 3(1)(h)(v); Commonwealth PPI Bill, s 4; Commonwealth Privacy Bill, s 4.

127 Explanatory Report to Convention 108+, para 60 p. 22

128 HIPCAR Model Legislative Text, s 3(2)(a)(iv); OAS Principles with Annotations, Definitions, Page 7 (definition of sensitive personal data).

129 AU Convention, art 1; GDPR, art 4(15), recital 35; HIPCAR Model Legislative Text, s 3(1)(h), s 3(1)(h)(v); Explanatory Report to Convention 108+, para 60 p. 22.

130 AU Convention, art 1; GDPR, art 4(15), recital 35; Convention 108+, Explanatory Report, para 60 p. 22.

Health data is information that relates to the physical or mental health of an individual. It includes all types of data related to health status and services, treatment choices, plans and reports, health security or policy numbers, as well as socio-economic parameters regarding health and well-being. Data gathered as a result of managing a healthcare system, providing healthcare services, or conducting health research is considered as health data.¹³¹ Clearly, all personal data having clear and close links to information relating to an individual's health status is also covered under the concept of health data.¹³² It would include medical or clinical data, administrative data and financial data related to health, and personal health policy information within the health sector.¹³³ For instance, when the purpose of the application is to monitor the health or well-being of the individual, it does not matter whether it is in a medical context or otherwise.

The GDPR, Convention 108+, AU Convention and the HIPCAR Privacy Framework cover both physical and mental health-related data.¹³⁴ In addition, the GDPR and Convention 108+ also clarify that such information may relate to the individual's health status at different points of time in the past, present, and future.¹³⁵ The GDPR also covers information collected for the purpose of providing health care services that reveals an individual's health status.¹³⁶ It considers personal data concerning health to include: (i) information that uniquely identifies the concerned person for health purposes; (ii) information derived from biological testing/samples such as genetic data; (iii) information related to any disease and associated risks, disability, and medical history; and (iv) clinical treatment or the physiological or biomedical state of an individual. It also clarifies that such information may be derived "independent of its source," such as from "physicians

or other professionals, hospitals, medical devices or in vitro diagnostic tests."¹³⁷

Although the GDPR and the HIPCAR Privacy Framework consider health data as sensitive data, they allow its processing in certain situations. The GDPR permits processing of health data under necessary circumstances, such as for preventive or occupational medicine, assessment of an employee's working capacity, medical diagnosis, and for the public interest of the healthcare sector.¹³⁸ The HIPCAR Privacy Framework makes exemptions for national security and health management purposes.¹³⁹ It allows 'health care professionals' and 'health care institutions' to process health information without the requirement of consent.¹⁴⁰ The HIPCAR Privacy Framework defines the terms "health care professional" and "health care institution" and emphasises the need to appropriately define these terms "as they form a recurrent basis for non applicability of the law" with respect to the data subject's consent for the purpose of collection, processing and disclosure of personal information.¹⁴¹ It explains that the basis of providing the exemption is to ensure "that the data protection framework does not hamper the natural operation of such services".¹⁴²

131 'What is Health Data' (IGI Global) <https://www.igi-global.com/dictionary/health-data/42215> .

132 European Data Protection Supervisor, 'EDPS opinion on patients' rights: specific data protection dimension of cross-border healthcare needs to be addressed in more concrete terms' (Brussels, 3 December 2008) https://edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2008-12_patients_rights_en.pdf.

133 European Data Protection Supervisor, 'Prior-checking Opinion regarding the processing of health data at the European Insurance and Occupational Pension Authority (EIOPA) (EDPS case 2017-0284)' https://edps.europa.eu/sites/default/files/publication/18-05-23-opinion-eiopa-case-2017-0284_en.pdf.

134 GDPR, art 4(15); AU Convention, art 1; HIPCAR Model Legislative Text, s 3(1)(h)(v); = Explanatory Report to Convention 108+, para 60 p. 22.

135 GDPR, art 4(15); Explanatory Report to Convention 108+, para 60 p. 22.

136 GDPR, art 4(15).

137 GDPR, recital 35.

138 GDPR, art 9.

139 HIPCAR Model Legislative Text, s 15(3)(b), (e).

140 HIPCAR Model Legislative Text, s 15(3)(b).

141 HIPCAR Model Legislative Text, Section III, para 11.

142 HIPCAR Model Legislative Text, Section III, para 11.

2.5.2 Biometric Data

Biometric data is understood to be distinctive, measurable human characteristics that identify a person uniquely. They generally include fingerprints, face or iris scans, voice, DNA, and hand or body geometry.¹⁴³

Biometrics are increasingly being used for authorisation and security purposes including access control, monitoring, identification, and authentication by both public and private actors across sectors, such as banking and finance, healthcare, travel, social services, education, intelligence and crime detection. Emerging technological systems use human characteristics (such as gait, voice pattern and emotions); physiological traits (such as face, iris and fingerprints), and biological markers (such as DNA and blood) to assign unique identification and authentication methods.¹⁴⁴

While biometric systems may enhance user comfort, support development and humanitarian initiatives, and improve the efficiency of government intelligence operations and security, they also raise data protection challenges due to the sensitive nature of the information being collected and processed.¹⁴⁵ Many national and regional data protection frameworks distinctly regulate biometric data to protect data subject rights. Of the Identified Regional Frameworks, the GDPR and the Convention 108+ define the term “biometric data”.¹⁴⁶

The GDPR and the Convention 108+ differ subtly when it comes to biometric data. While both include personal data relating to physical or physiological

characteristics of a natural person, the GDPR also makes use of behavioural characteristics, which include analysis of unique patterns such as handwritten signature, gait, and gaze.¹⁴⁷ On the other hand, Convention 108+ refers to biological characteristics,¹⁴⁸ which are based on genetic and molecular markers.

Both the GDPR and Convention 108+ mark biometric data that uniquely identifies an individual as a special category of data/sensitive data.¹⁴⁹ The Explanatory Report to Convention 108+ notes that biometrics touch upon the “most intimate sphere” of a data subject’s life and could affect crucial outcomes concerning the subject, such as their physical safety, dignity, and guilt or innocence in criminal proceedings.¹⁵⁰

The GDPR and Convention 108+ both limit the scope of biometric data to personal data resulting from specific technical processing that uniquely identifies and authenticates an individual.¹⁵¹ The definition excludes raw biometric data,¹⁵² such as facial images, video footage, voice recordings or fingerprints stored or retained in databases that have not undergone “processing using specific technical means.” Therefore, raw biometric data does not come within the ambit of sensitive or special data despite being biometric data from a strictly technical standpoint. Nevertheless, such data constitutes personal data. However, if the processing of images reveals racial, ethnic or health related data, it will be considered as sensitive data.¹⁵³ For instance, processing images that have visible health characteristics (use of a wheelchair, broken leg, glasses) will be considered as processing sensitive data if it is based on health information extracted from the images.¹⁵⁴

143 Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies dated 27 April 2012 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

144 Fenu G and Marras M, ‘Leveraging Continuous Multi-Modal Authentication for Access Control in Mobile Cloud Environments’ in Sebastiano Battiato and others (eds), *New Trends in Image Analysis and Processing – ICIAP 2017* (Springer International Publishing 2017).

145 Alan Gelb and Julia Clark, *Identification for Development: The Biometrics Revolution*, Working Paper 315 Centre for Global Development https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf.

146 GDPR, art 4(14); Convention 108+, Explanatory Report, para 58.

147 GDPR, art 4(14).

148 Explanatory Report to Convention 108+, para 58 p. 22.

149 GDPR, art 9(1); Convention 108+, art 6(1).

150 Explanatory Report to Convention 108+, para 55 p. 21.

151 GDPR, art 4(14); Explanatory Report to Convention 108+, para 58 p.22.

152 Data that is biometric by nature but is not considered as biometric data from a legal standpoint as it has not undergone processing using specific technical means to uniquely identify a natural person.

153 GDPR, art 9, Explanatory Report to Convention 108+, para 59 p 22.

154 Explanatory Report to Convention 108+, para 60 p. 22.

The HIPCAR Privacy Framework subsumes biometric data within the definition of personal information.¹⁵⁵ Similarly, the Commonwealth PPI and Privacy Bills also refer to certain physiological and biological traits like fingerprints and blood type when defining personal information.¹⁵⁶ The AU Convention, while not defining biometric data, only allows processing of biometric data after obtaining permission from the national data protection authority.¹⁵⁷

2.5.3 Genetic Data

Genetic data is considered to be among the most sensitive forms of personal data. It relates to inherited or acquired genetic characteristics of an individual, acquired through DNA or RNA analysis.¹⁵⁸ It contains both health and non-health-related information about the individuals and their family members.¹⁵⁹ It can reveal information about disorders, diseases, susceptibility to specific illnesses, as well as help track a person's ethnic origins and identify genetic relationships between individuals. Hence, genetic data also provides personal information related to family members and relatives.

Of the Identified Regional Frameworks, only the GDPR and Convention 108+ expressly define the term genetic data.¹⁶⁰ The AU Convention refers to genetic data while defining health data and allows processing of “data involving genetic information and health research only after seeking permission from the national protection authority.”¹⁶¹

Both the GDPR and Convention 108+ treat genetic data as a special category of sensitive data.¹⁶² They define genetic data as personal data relating to the inherited or acquired genetic characteristics of a natural person, which result from an analysis of an

individual's biological sample.¹⁶³ Both frameworks consider analysis from other molecular or biological sources, such as chromosomal, DNA or RNA analysis, as well as analysis arising from any other element that would produce equivalent information, as genetic data.¹⁶⁴ Neither framework clarifies whether genealogical information gathered through questionnaires would be considered as information derived from an “analysis of any other element” providing equivalent information as the analysis from a biological sample.¹⁶⁵

The peculiar characteristics of genomic information can enable scientific advances and create insights about an individual's health or predisposition to disease. However, processing genetic data for these purposes also creates tensions with the principles of data minimisation, anonymisation, and deletion.¹⁶⁶ Nevertheless, the current definition of genetic data provides a good starting point with scope for improvement to adapt to present and future developments.

155 HIPCAR Model Legislative Text, s 3(1)(h)(vi).

156 Commonwealth PPI Bill, s 3(1)(h); Commonwealth Privacy Bill, s 4.

157 AU Convention, art 10(4)(d).

158 Convention 108+, Explanatory Report para 57.

159 Shabani M and Borry P, ‘Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation’ (2018) 26 *European journal of human genetics*: EJHG 149.

160 GDPR, art 4(13); Convention 108+, art 6 Explanatory Report para 57.

161 AU Convention, arts 1, 10(4)(a).

162 GDPR, art 9; Convention 108+, art 6.

163 GDPR, art 4(13); Convention 108+, Explanatory Report para 57.

164 GDPR, art 4(13) read with recital 34; Convention 108+, Explanatory Report para 57.

165 Chassang G, ‘The Impact of the EU General Data Protection Regulation on Scientific Research’ (2017) 11 *ecancermedicalsecience* 709.

166 Colin Mitchell, Johan Ordish, Emma Johnson, Tanya Brigden and Alison Hall, ‘The GDPR and genomic data: The impact of the GDPR and DPA 2018 on genomic healthcare and research’ (PHG Foundation, May 2020) 58 <<https://www.phgfoundation.org/media/123/download/gdpr-and-genomic-data-report.pdf?v=1>>.

2.6 Controller and Processor

Controllers and processors play a crucial role in the operationalisation of data protection law. Both engage in processing the personal data of data subjects. Hence, it is important to clearly delineate their responsibilities, obligations, and liabilities within the data protection framework. The framework must make it incumbent on the controller and processor to implement data protection principles, such as accountability and transparency, confidentiality, and integrity to protect and secure the personal data and rights of the data subjects. The definition of a controller or processor determines which entities are bound by the obligations set out by the data protection framework.

Under the Identified Regional Frameworks, typically, a controller is either: a natural or legal person, a private organisation, association, entity, or body, or a public authority or body.¹⁶⁷ The inclusion of public agencies or authorities as controllers ensures that data protection principles apply to the processing of data by the state and its various bodies. Some frameworks do not use the term controller and simply place obligations on organisations that carry out data processing.¹⁶⁸ The controller is responsible for processing personal data and holds decision-making powers with regards to processing of the personal data. It determines the purpose and manner of personal data processing, either alone or jointly,¹⁶⁹ and is also responsible for

compliance with organisational, technical and security measures along with the data protection principles.¹⁷⁰ Similarly, a processor is either: a natural or legal person, a private organisation, association, entity, or body, or a public authority or body.¹⁷¹ Crucially, the processor undertakes processing of personal data on behalf of the controller.¹⁷² The processor is under an obligation to comply with the scope of processing and assist and facilitate the controller's organisational, technical and security measures,¹⁷³ and must inform the controller in case of a breach.¹⁷⁴ A processor is usually an entity or third party outside the controller's organisation.¹⁷⁵ An employee of the controller cannot be considered as a processor.¹⁷⁶

2.6.1 Controllers

Of the Identified Regional Frameworks, the APEC Privacy Framework, the AU Convention, the GDPR, the HIPCAR Privacy Framework, the OAS Principles, and Convention 108+ provide an explicit definition of the term controller.¹⁷⁷ Others, such as the ASEAN DP Framework, Commonwealth PPI and Privacy Bills do not define the term, but refer to entities or persons processing personal data.¹⁷⁸ The AU convention, GDPR, OAS Principles, Convention 108+, Commonwealth Privacy Bill expressly allow public authorities to be identified as data controllers and

-
- 167 APEC Privacy Framework, part ii, para 10; AU Convention, art 1 (definition of data controller); GDPR, art 4(7); OAS Principles with Annotations, Definitions, page 6 (definition of data controller); Convention 108+, art 2(d); Commonwealth Privacy Bill s 4 (definition of public authority); Commonwealth PPI Bill, s 5(1) (use of 'organisation').
- 168 ASEAN DP Framework, para 6(a) (use of the term 'organisation'); Commonwealth PPI Bill, s 3.
- 169 AU Convention, article 1 (definition of data controller); GDPR, art 4(7); HIPCAR Model Legislative Text 3(1)(c); OAS Principles with Annotations, Definitions, page 6 (definition of data controller); Convention 108+, art 2(d).
- 170 GDPR, arts 5(2), 24; AU Convention, art 13 (principle 6(b)).
- 171 GDPR, art 4(8); OAS Principles with Annotations, Definitions, page 6 (definition of data processor); Convention 108+, art 2(f).
- 172 GDPR, art 4(8); Convention 108+, art 2(f); HIPCAR Model Legislative Text, s 14.
- 173 AU Convention, art 13 (principle 6(b)); GDPR, art 28(3).
- 174 GDPR, art 33(2).
- 175 OAS Principles with Annotations, Definitions, page 6 (definition of data processor).
- 176 Convention 108+, Explanatory Report para 24.
- 177 APEC Privacy Framework, part ii, para 10; AU Convention, art 1 (definition of data controller); GDPR, art 4(7); HIPCAR Model Legislative Text, s 3(1)(c); OAS Principles with Annotations, Definitions, page 6 (definition of data controller); Convention 108+, Art 2(d); OECD Guidelines, Chapter 1, Part 1, para 1(a).
- 178 ASEAN DP Framework, para 6; Commonwealth PPI Bill, s 5(1); Commonwealth Privacy Bill, s 3.

regulate their processing of personal data.¹⁷⁹

All the regional frameworks that define a data controller agree that the controller has decision-making power with respect to data processing.¹⁸⁰ It is an entity that decides the contents and use of personal data.¹⁸¹ It includes a person or organisation that instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information on their behalf. However, controllers may also themselves collect and process data.¹⁸²

The ECJ has analysed whether Google, a search engine, is a controller by virtue of processing personal data, which was uploaded on its website without its knowledge; and found that since Google was the entity determining the purposes and means of personal data processing, it should be considered as a data controller.¹⁸³

Citing this case, Facebook, and the administrator of a Facebook fan page, were also declared as data controllers in another case.¹⁸⁴ In another landmark case, the ECJ determined that a website operator featuring the Facebook ‘Like’ button, would be a joint controller of personal data under the GDPR.¹⁸⁵ However, the Court limited the website operator’s liability to its role in collecting and transmitting personal data to Facebook, and not for any subsequent data processing carried out by Facebook.

“All the regional frameworks that define a data controller agree that the controller has decision-making power with respect to data processing.”

179 AU Convention, art 1 definition of data controller); GDPR, art 4(7); HIPCAR Model Legislative Text s 3(1)(c) (definition of data controller) read with Part IV; OAS Principles with Annotations, Definitions, page 6 (definition of data controller); Convention 108+, Art 2(d), Commonwealth Privacy Bill, s 6.

180 OAS Principles with Annotations, Definitions, page 6 (definition of data controller); APEC Privacy Framework, part ii, para 10; AU Convention, art 1 (definition of data controller); GDPR, art 4(7); HIPCAR Model Legislative Text, s 3(1)(c) (definition of data controller); Convention 108+, art 2(d); OECD Guidelines, Chapter 1, Part 1, para 1(a).

181 OAS Principles with Annotations, Definitions, page 6 (definition of data controller); GDPR, art 4(7); Convention 108+, art 2(d); AU Convention, art 1 definition of data controller); HIPCAR Model Legislative Text s 3(1)(c) (definition of data controller).

182 OAS Principles with Annotations, Definitions, page 6 (definition of data controller).

183 Google Spain SL v AEPD (The DPA) and Mario Costeja Gonzalez, Case No C-131/12 decision dated 13 May 2014 <https://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd?searchuniqueid=7211620>.

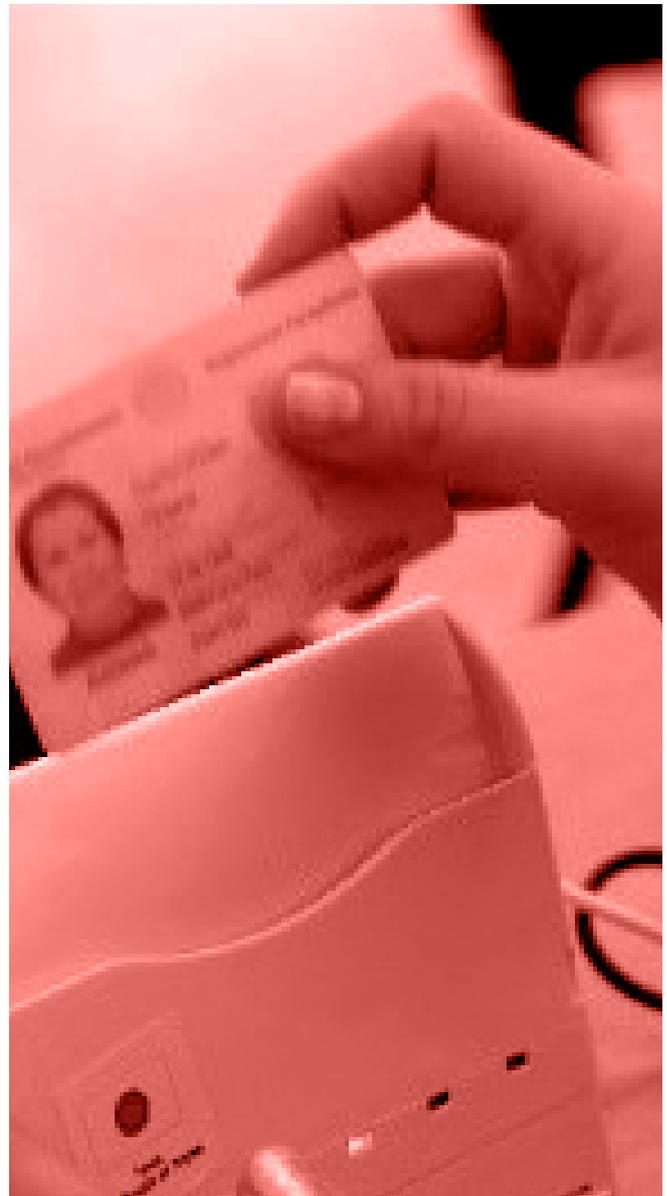
184 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein, Case C-210/16 decision dated 5 June 2018.

185 Fashion ID GmbH and Co KG v Verbraucherzentrale NRW eV Case C-40/17 decision dated 29 July 2019 (paras 75-83).

2.6.2 Processors

The GDPR, the OAS Principles, and Convention 108+¹⁸⁶ are the only instruments amongst the Identified Regional Frameworks that define a data processor. However, the AU Convention, the HIPCAR Privacy Framework, and the OECD Guidelines refer to processors indirectly. They speak of entities undertaking processing on behalf of a controller that will duly comply with security measures.¹⁸⁷ The AU Convention and HIPCAR Privacy Framework make it incumbent on a controller to select a processor that can ensure a level of data protection consistent with the framework.¹⁸⁸

Likewise, the GDPR also requires controllers to delegate processing to processors that are able to provide data protection guarantees.¹⁸⁹ The GDPR clarifies that although a processor can make its own operational decisions, it must strictly adhere to the controller's instructions¹⁹⁰ when processing data, as well as comply with the framework.¹⁹¹ The controller may provide a certain degree of discretion to the processor to choose the most suitable technical and organisational means to process the data. However, broadly speaking, the processor is required to act "on behalf of" the controller and cannot carry out processing except as instructed by the controller.¹⁹² When a processor goes beyond the controller's instructions and starts determining its own purposes and means of processing, it would be considered as a controller.¹⁹³ In such cases, the responsibilities and liabilities of a data controller will become applicable to the processor. Additionally, the processor may face sanctions from the controller for bypassing the controller's instructions.¹⁹⁴



186 GDPR, art 4(8); Convention 108+, art 2(f); OAS Principles with Annotations, Definitions, Page 6.

187 AU Convention, art 13 (Principle 6(b)); HIPCAR Model Legislative Text s 14(2); OECD Guidelines, Chapter 2, Page 23.

188 AU Convention, art 13, Principle 6(b); HIPCAR Model Legislative Texts 14.

189 GDPR, art 28(1).

190 GDPR, art 29.

191 GDPR, art 28.

192 GDPR, art 29.

193 Case C-40/17 decision dated 29 July 2019(para 79).

194 GDPR, art 82(2).

Key considerations and summary points

- ◇ The scope of the 'personal data' definition determines which type of data will be regulated by a data protection framework.
- ◇ Most modern frameworks rely on the concept of identifiability which defines personal data as data that can directly or indirectly identify an individual. Several frameworks provide lists of identifiers and factors that would cause individuals to be identified through data.
- ◇ Broad definitions of personal data ensure the most protective and future-proof approach, which allows courts and data regulators the opportunity to protect individuals in the face of changing technologies.
- ◇ De-identification methods attempt to reduce or eliminate the possibility that data identifies individuals.
- ◇ Processes such as anonymisation break the link between datasets and individuals, rendering them non-identifiable. Because anonymous data is often exempt from data protection requirements, however, legislation should ensure that re-identifying anonymised data is 'reasonably' difficult or impossible.
- ◇ Pseudonymised data can be reidentified and therefore continues to be governed by data protection frameworks.
- ◇ Data subjects are individuals whose data is processed and are the primary beneficiaries of data protection frameworks.
- ◇ Data subjects are typically living, natural persons, although in certain situations, the benefits of data protection frameworks may be extended to deceased and legal persons.
- ◇ Health data covers data related to the past, present, and future physical or mental health of a data subject, including treatment plans, reports, health expenditure, and disease risk. Health data is often treated as a special category of data, subject to enhanced data protection safeguards.
- ◇ Biometric data refers to distinctive and measurable characteristics of data subjects, such as fingerprints and body geometry. It is typically treated as a special category of sensitive data with additional safeguards, as it is intimately related to the data subject's identity and could impact them significantly (e.g., during criminal proceedings).
- ◇ Genetic data concerns inherited or acquired genetic characteristics of data subjects acquired through DNA or RNA analysis. Like health and biometric data, it is typically treated as a special category of sensitive data by legal frameworks.
- ◇ The definition of a data controller and data processor determine which public and private entities are subject to the obligations of a data protection framework.
- ◇ Data controllers determine how and for what purposes data is processed. Controllers must therefore demonstrate compliance with the data protection framework.
- ◇ Data processors are entities which process data on behalf of controllers. Data processors must comply with the controller's instructions and any other obligations imposed on processors by the data protection framework.
- ◇ Ensuring that public agencies and the state itself are treated as data controllers ensures that key data protection principles apply to the processing of citizens' information by the relevant public institutions.

CHAPTER 3

ESTABLISHED DATA PROTECTION PRINCIPLES



3.1 Introduction

This chapter draws on the Identified Regional Frameworks to discuss the data protection principles that should be incorporated within domestic legislation. This includes the principles to be followed by data controllers, such as government agencies or private companies, when collecting, processing, and using personal data. Technical mechanisms to achieve optimum data privacy, such as the concept of privacy by design, are discussed in Chapter 4 (Transparency and Accountability).

Multilateral organisations have observed that the state's use of digital technologies to confer legal identity or verify the identities of its citizens and resident foreigners is a powerful tool to achieve the SDG goal of providing legal identity for all.¹⁹⁵ However, these initiatives raise certain concerns for citizens' privacy rights, in particular for their informational privacy.¹⁹⁶ With numerous countries across the world implementing digital ID systems (e.g. Argentina, Estonia, India, Malawi, Senegal, Uganda),¹⁹⁷ ¹⁹⁸ questions concerning privacy and the use of personal data must be addressed by introducing legal safeguards to adequately protect individuals and ensure state accountability.

In the absence of a robust data protection law, the personal data of citizens may be vulnerable to misuse.

A strong data protection regime must be based on clear principles governing the processing, storing and sharing of data.

The last decade has witnessed several high profile incidents when personal data has been illegitimately used by both private and public actors, which has accelerated the demand for robust data protection laws. The consulting firm Cambridge Analytica, for example, purchased large amounts of personal data about American citizens from Facebook without their knowledge, in order to allegedly influence voting behaviour during the 2016 US elections.¹⁹⁹

As an example of governmental digital response to the COVID-19 pandemic, Israel's contact tracing app relied on collecting metadata from voice calls,

195 World Bank, Principles on Identification for Sustainable Development (2021) <https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf>; UN Legal Identity Agenda Task Force, 'UN Strategy for Legal Identity for All' (June 2019), para 26 <https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf>.

196 See Reetika Khera, 'Impact of Aadhaar on Welfare Programmes' (2017) 52 (50) EPW <https://dx.doi.org/10.2139/ssrn.3045235>.

197 CIVIPOL Project, Senegal: Support Programme to Strengthen the Civil Registration Information System and Consolidation of a National Biometric Identification Database < <https://www.civipol.fr/en/projects/senegal-support-programme-strengthen-civil-registration-information-system-and>; National Identification and registration Authority, Uganda <https://www.nira.go.ug/>; Calum Handforth and Matthew Wilson, 'Digital Identity Country Report, Malawi' (GSM Association, 2019) <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf>; World Bank Group, Argentina ID Case Study: The Evolution of Identification (2020) <https://olc.worldbank.org/system/files/Argentina-ID-Case-Study-The-Evolution-of-Identification.pdf>.

198 National Identification Authority, Republic of Ghana <https://nia.gov.gh/>; Huduma Namba, Republic of Kenya; National Identity Management Commission, Nigeria; World Bank Group, 'ID4D Country Diagnostic; Ethiopia' (2017) <https://documents1.worldbank.org/curated/en/822621524689442102/ID4D-Country-Diagnostic-Ethiopia.pdf>.

199 Issie Lapowsky, 'How Cambridge Analytica Sparked the Great Privacy Awakening' (Wired, 17 March 2019) <<https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>>.

text messages and browsing histories.²⁰⁰ In light of these events, several nations are in the process of introducing new data protection laws or overhauling existing ones. Brazil is developing and adopting new data protection legislation,²⁰¹ while the EU's GDPR is now applicable across borders to any entity that offers its goods and services to EU residents.²⁰² A data protection framework is also being debated in India.²⁰³ The US state of California,²⁰⁴ and the countries of Nigeria and Kenya have also drawn inspiration from the GDPR and recently updated their privacy laws.²⁰⁵ In keeping with this trend, several nations have also participated in the creation of regional data protection instruments that reflect the growing consensus among states of the importance of data protection.

Despite differences in legal traditions and sociocultural values, several regional data protection and privacy frameworks provide for certain core rules or principles that domestic data protection legislation should include.²⁰⁶ Known as data protection principles, or core privacy principles, these set out the approach that data controllers and processors ought to incorporate when processing personal data and designing their systems and controls. Incorporated across all the Identified Regional Frameworks the principles include legal, management, administrative, and technical safeguards.



- 200 Tehilla Shwartz Altshuler and Rachel Aridor Hershkowitz, 'How Israel's COVID-19 mass surveillance operation works' (Brookings, 6 July 2020) <https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/>.
- 201 The General Personal Data Protection Law 13709/2018 is a statutory law on data protection and privacy in the Federative Republic of Brazil http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.
- 202 Regulation (EU) 2016/679 of 27 April 2016 addresses the transfer of personal data outside the EU and EEA areas [2003] OJ L 119/1.
- 203 Report of the Joint Committee on the Personal Data Protection Bill, 2019 available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.
- 204 California Consumer Privacy Act, 2018 gives consumers more control over the personal information that businesses collect about them. California Consumer Privacy Act 2018 https://leginfo.ca.gov/faces/codes_display_Text.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.
- 205 Brian Daigle, 'Data Protection Laws in Africa: A Pan-African. Survey and Noted Trends'2021 (Journal of International Commerce and Economics11 https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf.
- 206 David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books, 2014).

Box 3.1: Key principles adopted by the European Union and OECD

The EU's and OECD's approaches to data protection provide useful starting points for countries working to develop data protection frameworks and represent nearly four decades of engagement with the issue of data protection.

The EU's GDPR is a comprehensive data protection framework that has helped set new thresholds for privacy standards. Article 5 sets out the core principles that data controllers and processors are required to adopt. These principles require personal data to be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes;
- adequate, relevant, and limited to what is necessary for the purposes it was processed for;
- accurate and, where necessary, kept up to date;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, and;
- processed in a manner that ensures appropriate security of the personal data.

The OECD Guidelines have been accepted as an international standard for personal information processing principles. The Guidelines set out the following eight principles with respect to data collection and processing:

- **Collection Limitation** – data collection should only occur with the prior knowledge and consent of the data subject.
- **Data Quality** – data controllers and processors should only collect personal data which is relevant and accurate for a particular aim.
- **Individual Participation** – the concerned individual should know if their personal data has been collected and must be able to access such collected data.
- **Purpose Specification** – the intended use for a particular piece of information must be known at the time of collection.
- **Use Limitation** – collected data must not be used for purposes other than the ones specified at the time of collection.
- **Security Safeguards** – reasonable measures must be taken to protect data from unauthorised use, destruction, modification, or disclosure of personal data.
- **Openness** – individuals should be able to establish that data collection has occurred and be able to contact the entity collecting this information.
- **Accountability** – data collectors should be held accountable for failing to abide by any of the above principles.

The remainder of this chapter analyses the specific principles found in the Identified Frameworks including: (i) that processing be fair, lawful, and transparent; and the principles of (ii) notice and consent; (iii) purpose limitation; (iv) data minimisation; (v) data accuracy; (vi) and integrity, confidentiality and availability; and (vii) transparency and accountability.

3.2 Fair, lawful and transparent

“It is critical that data controllers and processors demonstrate their compliance with data protection laws and principles when collecting and processing personal data.”

It is critical that data controllers and processors demonstrate their compliance with data protection laws and principles when collecting and processing personal data. This ensures that data subjects enjoy their right to privacy and can seek legal redress for any infringement of their rights. To ensure this, frameworks such as the GDPR and OECD mandate that data controllers and processors abide by the principles of fairness, lawfulness and transparency in data processing activities.²⁰⁷

The principle of lawfulness is often applied in conjunction with the principles of fairness and transparency that require data controllers and processors to process the personal data of data subjects only after providing adequate notice to the data subject in a format that is concise, easily accessible, easy to understand, in clear and plain language and in a manner that is fair.²¹¹

A data controller or processor must provide a privacy notice that sets out how an organisation collects, uses, retains, and discloses personal data. This notice must clearly inform users of the ways in which their personal data will be used and managed, along with the legal grounds or bases for doing so.²¹² Such processing should keep in mind the best interests of the data subjects and must not be harmful, discriminatory, deceptive, misleading or unexpected.²¹³ Furthermore,

207 GDPR, art 5(1); OECD Guidelines, Chapter 1, paras 7, 9, 10-12.

211 Damian Clifford, Jef Ausloos, ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130–187 <https://doi.org/10.1093/yel/yey004>.

212 F. H. Cate and V. Mayer-Schonberger, ‘Notice and Consent in A World Of Big Data’ (2013) 3 International Data Privacy Law.

213 See Daniel-Mihail Sandru, ‘The Fairness Principle in Personal Data Processing’ (2020) 10(1) Law Review <http://dx.doi.org/10.2139/ssrn.3641883>.

Box 3.2: What is fairness, lawfulness, and transparency?

What is fairness?

In general, fairness means that data controllers and processors should only handle personal data in ways that data subjects would reasonably expect and not use it in ways that could potentially have any unforeseen or adverse effects on them. For example, a default setting in software that leads to unexpected sharing of personal computer files was held to be unfair by a US court because it hindered consumer choice.²⁰⁸ Similarly, the French data protection authority, la Commission nationale de l'informatique et des libertés (CNIL), sanctioned Les Pages Jaunes (Yellow Pages) for collecting information about individuals from their public social media profiles and then aggregating that information in Les Pages Jaunes' online directory service.²⁰⁹ The CNIL found the processing unfair (déloyal) because data subjects were not adequately informed that information about their public profiles would be collected by Les Pages Jaunes. They were also not given an opportunity to grant informed consent.

What is lawfulness?

For the processing of personal data to be lawful, data controllers and processors must identify and determine the legal bases for processing different types of data. These bases may include specific purposes and contexts of processing. Frameworks such as the GDPR specifically outline legitimate grounds for processing data which include: the consent of the data subject;

- the performance of a contract;
- the performance of a task carried out in the exercise of an authority's compliance with a legal obligation;
- legitimate interests of the controller or third parties;
- the protection of the data subject's vital interests.²¹⁰

Lawfulness also refers to the requirement that data controllers and processors comply with statutory or other legal obligations whether they be criminal or civil. For example, data controllers and processors would be required to comply with corporate filing and disclosure requirements under company law and abstain from committing offences such as fraud or forgery that are prohibited by penal statutes.

What is transparency?

Transparent processing of personal data means being clear, open, and honest with data subjects about which entities constitute the chain of data controllers and processors and how and why they use the personal data.

208 In Re Sony BMG Music Entertainment, US FTC Matter 062-3019 (29 June 2007) Complaint.

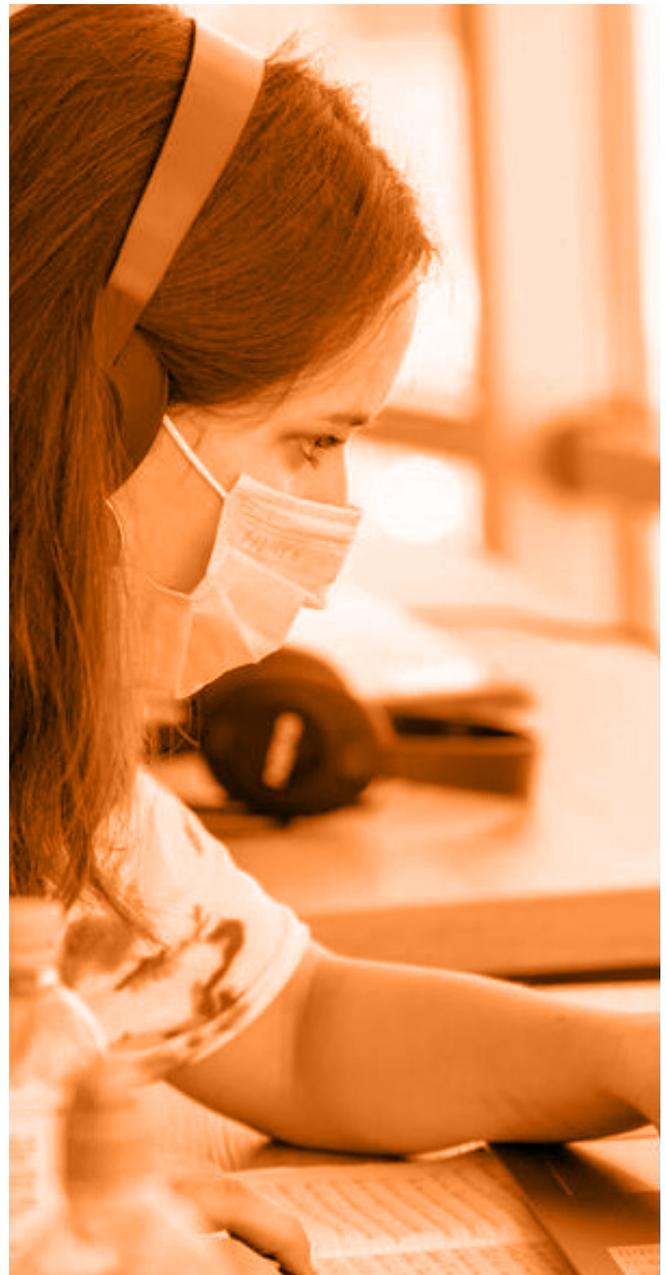
209 CNIL Deliberation 2011-203 of 21 September 2011 <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000024583206/>.

210 GDPR, art 6(1).

any subsequent changes to the uses of personal data must be communicated to the data subject prior to such use.²¹⁴

These principles assume greater importance when personal data is processed by the state or its agencies. The COVID-19 pandemic has seen governments use technological tools to contain the spread of infection and trace infected individuals. Many governments have justified the collection and processing of sensitive health data and other personal data as necessary to protect public health. However, this has led to the use of individuals' personal data in new and at times unexpected ways. Some countries have resorted to emergency measures to collect data from CCTV cameras, cell phones, and credit-card transactions in order to track potentially infected persons and their movements and interactions with other people.²¹⁵ As noted by the OECD, data collection and processing efforts should preferably be authorised by law and specify how such data collection and processing will be limited to a section of the population, for a limited time period, and solely for the purpose of combatting COVID-19.²¹⁶

Adherence to the principles of fairness, lawfulness, and transparency may help mitigate these adverse impacts. For example, states and health agencies can ensure that the data collected is strictly necessary for the stated purpose of responding to a public health emergency. Crucially, the data must not be used in any manner incompatible with the purpose of a public health response. The collection and processing of this data must also be disclosed to data subjects, and the data must not be retained for longer than necessary.



214 See GDPR, art 13(3).

215 Aditi Agarwal, 'Aarogya Setu Updated Its Privacy Policy: All You Need To Know' (Medianama, 14 April 2020) <https://www.medianama.com/2020/04/223-aarogya-setu-privacy-policy/>; Maya Wang, 'China: Fighting COVID-19 With Automated Tyranny' (Human Rights Watch, 1 April 2020) <https://www.hrw.org/news/2020/04/01/china-fighting-covid-19-automated-tyranny>; 'Israel uses surveillance tech to track coronavirus patients' (DW News, 20 March 2020) <https://www.dw.com/en/israel-uses-surveillance-tech-to-track-coronavirus-patients/av-52864272>; Aaron Holmes, 'Singapore is using a high-tech surveillance app to track the coronavirus, keeping schools and businesses open. Here's how it works.' (Business Insider, 24 March 2020) <https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3>; Douglas Busvine, 'Switzerland, Austria align with 'Gapple' on corona contact tracing' (Reuters, 22 April 2020) <https://www.reuters.com/article/health-coronavirus-europe-tech/switzerland-austria-align-with-gapple-on-corona-contact-tracing-idUSL3N2CA36L>.

216 OECD, Ensuring data privacy as we battle COVID 19 (April 2020) <https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/>.

3.3 Notice and consent

Most legal and regulatory approaches to protecting informational privacy rely on obtaining informed consent as a lawful basis to limit how the personal information of a data subject can be collected or processed.²¹⁷ Among international frameworks, consent-based privacy management provisions can be found in the GDPR, APEC Privacy Framework, ASEAN DP Framework, HIPCAR Privacy Framework, OAS Principles, Commonwealth PPI Bill, and OECD Guidelines.²¹⁸ For decades, legislation has required that data subjects be informed about what types of data are being collected and how their information will be used by data controllers. This information is generally provided through privacy policies. These policies allow data subjects to exercise control over their data and provide consent based on their understanding of the privacy policy or notice shared with them prior to their data being collected. However, the notice-and-consent mechanism has its limitations and has been criticised on several grounds, described below.

to make informed decisions about their personal data.²²⁰ Given that privacy notices come in various forms, such as documents posted on websites, click-wrap agreements in software, signs posted in public spaces informing individuals about surveillance, a lack of access to such notices in a concise, intelligible format makes it challenging for individuals to provide meaningful consent. Furthermore, the lack of digital literacy among diverse populations as well as language barriers prevent data subjects from adequately understanding privacy policies in order to exercise effective control over their data and anticipate the consequences of their consent.

3.3.1 Consent fatigue

With individuals increasingly availing themselves of online products and services in the digital world, consenting to numerous privacy notices and policies may result in what is known as ‘consent fatigue’, or diminished consent, whereby one agrees to the privacy notice and provides consent without effectively comprehending the details and consequences of the privacy policy.²¹⁹ Additionally, privacy policy documents are often long and complicated, consisting of legal jargon which is changed frequently and is also beyond the reasonable understanding of an ordinary individual, making it challenging for them

217 Bailey R and others, ‘Disclosures in Privacy Policies: Does “Notice And Consent” Work?’ (National Institute of Public Finance and Policy, 2018) https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf.

218 GDPR, art 6(1), 7; APEC Privacy Framework, part iii, para 21-24; ASEAN DP Framework, principle 6(a); HIPCAR Model Legislative Text, s 9(1); OAS Principles with Annotations, principle 2; Commonwealth PPI Bill, s 8; OECD Guidelines, Chapter 1 OECD Privacy Framework, para 7.

219 Daniel S, ‘Introduction: Privacy Self-Management and The Consent Dilemma’ (2013) 126 Harvard Law Review; Aaron Smith, ‘Half of Online Americans Don’t Know what a Privacy Policy Is’ (Pew Research Center, 4 December 2014) <https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>.

220 Aleecia M. McDonald and Lorrie Faith Cranor, ‘The Cost of Reading Privacy Policies’ (2008) 4(3) ISJLP.

3.3.2 Power asymmetry

The principle of informed consent is based on the idea that individuals should be able to voluntarily make decisions concerning their exposure to potential dangers. The principle emphasises the importance of individual autonomy and responsibility for balancing risks and benefits.²²¹ In the context of data protection, informed consent refers to such consent that is freely-given, specific, unambiguous and revocable. For example, the APEC Privacy Framework calls on data controllers to provide data subjects with a “clear, prominent, easily understandable, accessible and affordable mechanism to exercise choice in relation to the collection, use and disclosure of their personal information” to ensure that individuals are provided with choice in relation to the collection, use, transfer and disclosure of their personal information.²²²

However, requiring individuals to consent to a data controller’s data practices based on privacy notices places the onus on an individual to be aware of the terms of data practices to which they are giving their consent, which benefits data controllers more than data subjects. This amplifies the power asymmetry between the user and the data controller, and undermines user empowerment.²²³ In some instances, such as in the context of employment or when personal data is required to be given to public authorities, consent may not always be given freely. This puts data subjects in a vulnerable position and may be especially challenging when the data controller is the state and has the power to deny persons access to benefits and public resources.

3.3.3 Opt-out mechanisms and the illusion of choice

Most traditional frameworks give data subjects the option to opt-out of providing consent for the collection and processing of their personal data.²²⁴ But when consent is revoked or withheld by data subjects, data controllers and processors can stop providing their services. This leaves data subjects with no option but to give consent if they want to avail themselves of specific services. Moreover, given the ubiquity of personal data collection at several points when consent and personal data are mandatory for access to services, opt-out mechanisms are impractical and, in some cases, impossible. In our networked society, where connectivity is essential for participation in modern life, the choice to withdraw completely is challenging. In such a scenario, the benefits of being connected may outweigh the drawbacks of privacy erosion.²²⁵

Taken together, the shortcomings discussed above make it clear that existing notice-and-consent mechanisms in privacy regulations are insufficient to meet the standard of informed consent. Countries worldwide are realising the challenges stemming from new technologies, such as artificial intelligence, machine learning, and big data that collect as much data as possible and retain such data for undisclosed, ambiguous, and potentially unethical purposes.²²⁶ Legislation is now relying on a rights-based model, wherein the burden of assessing the privacy risk to personal data is placed on the data controller, thereby obligating the data controller to be transparent of, and accountable for, its data collection, processing, transfer and storage.²²⁷

-
- 221 Bailey R and others, 'Disclosures in Privacy Policies: Does "Notice And Consent" Work?' (National Institute of Public Finance and Policy 2018) https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf.
- 222 APEC Privacy Framework, part iii, para 26.
- 223 Lorrie Faith Cranor, 'Necessary But Not Sufficient: Standardized Mechanism For Privacy Notice and Choice' (2012) 10 *Journal on Telecom and High Technology Law* http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Cranor.PDF.
- 224 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules'); Regulation (EU) 2016/679 (General Data Protection Regulation).
- 225 Lee Rainie, Janna Anderson, 'The Internet of Things Connectivity Binge: What Are the Implications' (Pew Research Center 6 June 2017) <https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/>.
- 226 Hervé A, "Data Protection and Artificial Intelligence" in Shin-yi Peng, Ching-Fu Lin and Thomas Streinz (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021)
- 227 OAS Principles with Annotations, principle 9 ("The burden should be placed on Data Controllers to assess the material risks to Data Subjects as part of the overall process of risk management and privacy impact assessment. Holding accountable whoever effectively exercises control over the Data will result in more meaningful protection of Data Subjects from material harm across a wide range of cultural contexts."). See also HIPCAR Model Legislative Texts, s 28; GDPR, section 3.

While data-driven private organisations are required to comply with numerous obligations prescribed within frameworks, governments or state agencies are often exempted from the purview of such regulations and are permitted to process personal data without the consent of data subjects when concerns regarding national security, defence, or public security are raised. The grounds for government access of personal data are discussed in more detail in Chapter 7 (Government Access). While these grounds are specified within regulations, critics argue that in the absence of clear definitions of terms such as national security, defence or public security, a state's power over individuals' personal data largely goes unchecked, leading to concerns of personal data misuse.²²⁸ Though countries such as Estonia, India, and Kenya require state actors to collect and process personal data in line with the principles of legality, necessity, and proportionality,²²⁹ the legal authorisation of such practices without appropriate oversight and safeguards can create risks, such as government-authorized surveillance and exclusion from government benefits and services.²³⁰

There is a growing need to develop and adopt new norms for notice-and-consent mechanisms that not only maximise access to data while ensuring transparency, but also protect each individual's right to control their informational privacy.²³¹ A human-centric approach towards this whereby the rights, needs, values, capabilities, and limits of data subjects are placed at the centre of any technological system, and risks are assessed prior to collection or processing of personal data is essential to fortify the digital privacy of individuals. Additionally, the rigorous implementation of other principles discussed in this chapter, such as fair and lawful use of data, purpose limitation, and privacy by design and as the default

can help mitigate the limitations of the notice and consent approach.

While notice and consent remains integral to a robust data protection framework, it must be supplemented by additional norms and safeguards to ensure consent is not rendered meaningless by issues such as consent fatigue and denial of services. However, many entities that collect and process personal data, including state actors and private organisations, benefit from the status quo and do not see any incentive to adopt practices that make data collection and processing more burdensome for them, but could potentially empower data subjects.²³²

“While notice and consent remains integral to a robust data protection framework, it must be supplemented by additional norms and safeguards to ensure consent is not rendered meaningless by issues such as consent fatigue and denial of services.”

-
- 228 Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee, 'Systematic government access to personal data: a comparative analysis' (2014) 4(2) International Data Privacy Law 96–119 <https://doi.org/10.1093/idpl/ipu004>.
- 229 Constitution and Personal Data Protection Act, 1996 (revised 2003 and 2008), Public Information Act, 2001 (last revised in 2018); Justice K. S. Puttaswamy (Retd.) v. Union of India and Ors. (2017) 10 SCC 1 <https://privacylibrary.ccglnud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uoi-and-ors?searchuniqueid=504175>; Okoiti v. Communications Authority of Kenya Constitutional Petition no.53 of 2017 [2018] eKLR <https://privacylibrary.ccglnud.org/case/okiya-omtatah-okoiti-vs-communication-authority-of-kenya-8-ors?searchuniqueid=995610>.
- 230 Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age (3 August 2018) UNGA A/HRC/39/29 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>; Prashant Agrawal, Anubhuti Singh, Malavika Raghavan, Subodh Sharma and Subhashis Banerjee, An operational architecture for privacy by design in public service applications, (December 2020), p 5, <https://www.dvara.com/research/wp-content/uploads/2020/12/An-operational-architecture-for-privacy-by-design-in-public-service-applications.pdf>.
- 231 Richard Warner & Robert Sloan, 'Beyond Notice and Choice: Privacy, Norms, and Consent' (2013) 14(2) J. High Tech. L.
- 232 'Redesigning Data Privacy: Reimagining Notice & Consent for human technology interaction' (World Economic Forum White Paper, July 2020) http://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

3.4 Purpose limitation

Data protection principles demand that personal data be processed only to the extent that is compatible with the purposes for which it was collected or subsequently consented to by the individual. This stems from the principle of ‘Purpose Limitation.’ Across data protection regimes, such as the APEC Privacy Framework, GDPR, Commonwealth PPI Bill, the HIPCAR Privacy Framework, and OECD Guidelines, the purpose limitation principle requires that personal data must be collected by data controllers “for specified, explicit and legitimate purposes” only.²³³ (Personal data must not be further processed in a way that is incompatible with the purposes for which it was collected.)

Broadly, the purpose limitation principle requires data controllers to carefully consider what purpose(s) the personal data will be used for and restricts them from collecting personal data which is not necessary, adequate or relevant for this intended purpose(s).²³⁴ Such intended purpose(s), which must be in accordance with law, should be communicated to data subjects at the point of collection in clear and unambiguous language so that individuals can determine what kind of processing is included within the specified purpose.²³⁵

The intention behind this principle is to ensure that data controllers are transparent, clear, and open from the outset about their proposed processing of personal data and the purposes are in line with data subjects’ reasonable expectations. Moreover, this principle becomes critical in today’s data-driven world when personal information of individuals, groups, and communities could be used for other objectives and

possibly have detrimental effects on individuals and lead to abuse.

However, several frameworks including the GDPR, the Commonwealth PPI Bill, HIPCAR Privacy Framework, and the OAS Principles also provide for exceptions to the purpose limitation principle whereby further processing of personal data is permissible with the consent of the data subject.²³⁶ Based on several examples around the world, it is also possible that the state and its agencies, in the exercise of their mandated functions, could share the personal data of their citizens with other state agencies. Therefore, any exceptions to the purpose limitation principle that permit further processing of data, especially by state agencies should be narrowly tailored and information sharing between state agencies tightly regulated.²³⁷ Otherwise, there exists a risk that the data subject’s consent is rendered meaningless.

233 GDPR art 5(1)(b). See also APEC Privacy Framework, part iii, para 25; Commonwealth PPI Bill, S 12(1); HIPCAR Model Legislative Text, S 7(b); OECD Guidelines, Chapter 1, Part 1, Para 9.

234 Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation (2 April 2013). See also GDPR art 5(1)(b); APEC Privacy Framework, part iii, para 25; Commonwealth PPI Bill, S 12(1); HIPCAR Model Legislative Text, S 7(b); OECD Guidelines, Chapter 1, Part 1, Para 9.

235 Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation (2 April 2013).

236 GDPR art 5(1)(b), art 6; Commonwealth PPI Bill, S 12(1); HIPCAR Model Legislative Text, s 15(1); OAS Principles with Annotations, principle 4.

237 See Privacy International, A Guide for Policy Engagement on Data Protection, page 39 <https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf>.

3.5 Data minimisation

At the core of privacy and data protection laws should lie the principle of data minimisation, which calls for limiting data collection to only what is required to fulfil a specific and legitimate purpose. When public and private organisations collect, process, and retain only the minimum necessary amount of personal data, it can limit privacy leakage and mitigate the risks associated with amassing large volumes of personal information. For example, an individual applying for a job should not be required to mandatorily disclose sensitive health information, such as their HIV status, unless it is required under certain reporting rules or to provide specific benefits. Since such information is not likely to be useful and could also result in potential discrimination, mandating the furnishing of such information could be excessive and in contravention of the data minimisation principle.

Data minimisation can be described as the principle of proportionality, necessity, non-excessiveness (or frugality) with respect to the quantity of personal data to be processed.²³⁸ The GDPR, the Personal Data Protection Guidelines for Africa, and the OAS Principles, as well as some domestic legislations, such as the California Consumer Privacy Act (US), and the Australian Privacy Act, 1988 limit personal data collected, processed or retained to the extent that it is relevant, required or necessary to accomplish the purposes specified.²³⁹ Such minimisation should be undertaken not only at the point of collection, but

should also apply to retention and the deletion of unnecessary data.²⁴⁰ Therefore, once the purpose for which data was collected has been fulfilled, data controllers must cease to store personal data. They must also subsequently delete the personal data unless required for any other specified purpose and consented to by the data subject. While frameworks do not specify what can be classified as adequate, relevant, and limited, data controllers must periodically review the amount and nature of personal data in its possession based on the circumstances of their intended processing operations.²⁴¹

In this regard, regulatory obligations imposed on data controllers and processors must determine and justify: (i) the nature of data collected on an ongoing basis; (ii) the legal basis for collecting such data; (iii) the purposes for which such data is collected; and (iv) the deletion of data that is no longer of any use. For example, the New York Department of Financial Services Cybersecurity Regulations mandated that regulated entities maintain a data minimisation program that calls for secure disposal of any non-public information that is no longer necessary for business operations and does not need to be maintained because of a legal or regulatory obligation.²⁴² Such regulatory supervision over data controllers and processors has enhanced the enforcement of the principle of data minimisation.²⁴³

238 Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) *Oslo Law Review* https://pdfs.semanticscholar.org/2abd/ebe58f95bce0bd6e605bbea808917caf4ef5.pdf?_ga=2.86142232.1863169313.1635746977-836047564.1635271278.

239 GDPR, art 25(1); The Internet Society and the Commission of the African Union, 'Personal Data Protection Guidelines for Africa' (19 May 2018) https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf; OAS Principles with Annotations, principle 3 ('relevance and necessity'); California Consumer Privacy Act, 2018 gives consumers more control over the personal information that businesses collect about them https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; The Privacy Act 1988, Schedule 1 (Australian Privacy Principles), principle 3 <https://www.oaic.gov.au/privacy/the-privacy-act/>.

240 OAS Principles with Annotations, principle 7 ('as per the 'minimization' and limited Processing and retention criteria, the processed Personal Data should correspond to the minimum required for the stated purpose and should not be kept for longer than necessary for such purposes').

241 Explanatory Report to Convention 108+, para 53.

242 New York State Department of Financial Services, 23 NYCRR 500, 500.13 (Limitations on Data Retention).

243 European Data Protection Board, 'Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company' (5 November 2019) [https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en#:~:text=On%20October%2030th%202019%2C%20the,Data%20Protection%20Regulation%20\(GDPR\).](https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en#:~:text=On%20October%2030th%202019%2C%20the,Data%20Protection%20Regulation%20(GDPR).)



The implementation of data minimisation supports “privacy or data protection by design and default” and requires data controllers and processors to integrate data protection and privacy features into their system engineering, practices, and procedures.²⁴⁴

To achieve data minimisation, data controllers and processors should adopt data minimisation measures, such as: use aggregate data when possible; pseudonymise personal data as soon as it is no longer necessary to have personally identifiable data; or anonymise or delete personal data once the purpose for which it was collected has been fulfilled.

244 OAS Principles with Annotations, principle 3 (‘Necessity and Proportionality’); GDPR, art 25.

3.6 Accuracy

As countries grapple with an unprecedented global health crisis, data has been an essential tool for crafting public policy responses to the pandemic, such as allocating resources, measuring the effectiveness of interventions (social distancing), and providing insights that can help lift movement restrictions and reopen economies. For example, data relating to infections, as well as medical resources such as the number of healthcare workers or available ventilators, has been useful in crafting healthcare responses across nations. Similarly, COVID-19 vaccine programmes have used public data sets such as census records to monitor vaccine hesitancy.²⁴⁵ Such information can ensure the delivery of life-saving services and benefits to thousands of people worldwide.

While technology-based solutions such as contact-tracing applications can be useful tools to address the challenges of the pandemic, the risk of bad data could have severe implications on the individuals that share their personal data with the state and other third parties, including violations of their human rights against discrimination and exclusion. For instance, inaccurate, incomplete, or unreliable data could have adverse effects on public health at large, as this data could obscure the needs of specific communities or socioeconomic realities, or even disinform populations. Policies reliant on inaccurate data may damage their effective implementation and fail to protect the public.

Given the nature of data that is continuously collected, processed, stored, updated, altered and transferred, data could potentially be damaged, raising concerns regarding the quality of data. For example, data can be damaged in transit when it is transferred from one network to another, or when any technical failure

corrupts data stored on a device. According to an MIT Sloan study, such inaccurate or corrupt data could cost businesses approximately 15 to 25 percent of their revenues.²⁴⁶ Therefore, there is a need to ensure data quality to build data subjects' trust in data collectors and processors and prevent any detrimental impact inaccurate data could have on businesses or operations or individuals. With accurate and reliable data, individuals and organisations can make the most informed decisions to protect the privacy of data subjects and, at the same time, be compliant with regulatory obligations. More importantly, keeping data updated and accurate reduces the costs associated with ineffective decisions and reduces the risks of inaccurate data. Data protection frameworks can ensure organisations maintain accurate and high quality data, most notably by granting individuals the right to access and correct data concerning them.²⁴⁷

Almost all the Identified Regional Frameworks governing data privacy, including APEC Privacy Framework, ASEAN DP Framework, GDPR, Convention 108+, the Commonwealth PPI Bill, OAS Principles, OECD Guidelines, and the HIPCAR Privacy Framework, incorporate the principle of data accuracy.

245 Lydia Anderson et al., 'New Tool Tracks Vaccination and Vaccine Hesitancy Rates Across Geographies, Population Groups' (United States Census Bureau, 21 April 2021) <https://www.census.gov/library/stories/2021/04/how-do-covid-19-vaccination-and-vaccine-hesitancy-rates-vary-over-time.html>.

246 Thomas C. Redman, 'Seizing Opportunity in Data Quality' (MIT Sloan Management Review, 27 November 2017) <https://sloanreview.mit.edu/article/seizing-opportunity-in-data-quality/>.

247 See Chapter 6 on the rights of data subjects.



3.7 Integrity, confidentiality, and availability

To secure personal data that is collected, processed, and stored on systems, and prevent unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data, entities are required to implement organisational and technical controls while handling personal data. These are typically in the form of encryption, authentication, and restricted access tools. Such controls form the organisation's security policy and generally focuses on protecting three key aspects of their data and information: confidentiality, integrity, and availability, which taken together form the core of information security and data protection. International and regional frameworks including the OECD, Convention 108+, and GDPR, mandate data controllers and processors to take necessary security measures against the risks discussed above by adopting reasonable security safeguards.²⁴⁸ These safeguards are directed at ensuring the confidentiality of data, its integrity and its availability.

3.7.1 Confidentiality

The objective of the confidentiality principle is to ensure that adequate data protection controls are in place to prevent any unauthorised or unlawful disclosure, access or use of data or damage, loss or destruction of data.²⁴⁹ Given that several members of staff within the organisation, as well as third parties, may be authorised to access certain data, such data should be made available on a “need to know” basis, with security controls that ensure that personal data stored is secure and kept private. Several measures such as using virtual private networks, enabling strong passwords or two-factor authentication, segregating data, and assigning privileges to restricted members of the organisation ensures data confidentiality. Based on the nature of data, data controllers and processors engaging with sensitive personal data such as health data or digital ID data should adopt stronger security controls.²⁵⁰

248 OECD Guidelines, Chapter 1, Part 2, para 11; Convention 108+, art 7(1); GDPR, art 32. See GDPR, art 5(1)(f); OAS Principles with Annotations, principle 6; Commonwealth PPI Bill, S 18; APEC Privacy Framework, part iii, para 28; HIPCAR Model Legislative Text, S 14.

249 World Bank, 'ID4D Practitioner's Guide: Version 1.0' (October 2019) <https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>.

250 Beck EJ, Gill W and De Lay PR, 'Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data' (2016) Global Health Action 9 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5123209/>; Olivia White et al, 'Digital identification: A key to inclusive growth' (McKinsey Global Institute, April 2019) <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx>.



3.7.1 Integrity

The principle of data integrity seeks to ensure the accuracy, trustworthiness, and validity of data throughout its lifecycle. Since information only holds its value as an asset to any organisation if it is accurate and complete, effective measures need to be taken to prohibit the alteration of data, whether stored in a system or in transit (such as with email) by unauthorised individuals or data processes. Towards this, organisations need to both ensure legitimate access to systems and prevent any unauthorised alteration or loss at the hands of those who have access to data. For example, to ensure that any lost data can be restored if altered, regular backups are essential to an organisation that holds critical information in its systems.²⁵¹ Similarly, organisations should also formulate policies that spell out access privileges and version controls to ensure the network's safety.

3.7.3 Availability

The compliance of this principle ensures that information on systems is readily accessible by authorised personnel when required. Given that organisations possess large volumes of data needed for business continuity, availability of, and uninterrupted access to, accurate data relies on the maintenance of hardware, software, equipment, and

communication channels that allow for the seamless storage and processing of data. Some of the most fundamental threats to availability are non-malicious in nature and include hardware failures, unscheduled software downtime and network bandwidth issues.²⁵² Conversely, malicious attacks include various forms of sabotage intended to cause harm to an organisation by denying users access to the information system. Popular methods adopted by organisations to ward against such threats include using proxy servers, access controls, and firewalls, ensuring adequate bandwidth, as well as backing up data and updating the systems at regular intervals, with some data backups possibly stored in foreign locations. Estonia, for instance, maintains an "out-of-border" backup of its citizens' data to ensure the continuity of operations in the event of an emergency.²⁵³ Additionally, organisations also adopt incident response plans to mitigate the risks associated with loss of data caused by breaches or unauthorised access to data.

251 John M. Borky, Thomas H. Bradley, 'Protecting Information with Cybersecurity' in *Effective Model-Based Systems Engineering* (Springer 2019) doi: 10.1007/978-3-319-95669-5_10.

252 Soila Pertet and Priya Narasimhan, 'Causes Of Failure In Web Applications' (2005) CMU-PDL-05-109 Parallel Data Laboratory Carnegie Mellon University <https://www.cs.cmu.edu/~priya/PDL-CMU-05-109.pdf>.

253 Peter Teffer, 'Estonia picks Luxembourg for 'ultimate backup'' (EU Observer, 30 June 2017) <https://euobserver.com/digital/138406>.

3.8 Transparency and accountability

These principles are covered in detail in Chapter 4 (Transparency and Accountability) below.

Key considerations

- ◇ A comprehensive and robust data protection legislation incorporates several key principles, such as: fairness; lawfulness; transparency and accountability; notice and consent; purpose limitation; accuracy; and integrity, confidentiality, and availability.
- ◇ The principle of lawfulness ensures that both private and public organisations' handling of personal data is governed by law.
- ◇ The principles of notice, consent, and transparency protect an individual's autonomy over their data and ensures that they are informed of how and when their data is collected. The principles of fairness and purpose limitation prevent collected data from being abused later in its lifecycle for unanticipated purposes.
- ◇ As private organisations collect increasing amounts of personal data and more states implement digital ID programmes, the principle of data minimisation attempts to limit the amount of data collected and processed, reducing the potential for leakages and misuse.
- ◇ The principles of accuracy, integrity, confidentiality, and availability impose obligations on controllers and processors to treat the data they do collect with a minimum standard of care to protect individuals from the harms arising from inaccurate or unavailable data, or the unauthorised access to data.



CHAPTER 4

MEASURES FOR TRANSPARENCY AND ACCOUNTABILITY



4.1 Introduction

The principles of transparency and accountability form an essential part of modern data protection law. The principles of transparency and accountability concern both compliance with data protection principles by data controllers and data processors, as well as the need to demonstrate this compliance.

Transparency and accountability measures in data protection laws typically require:

- adoption of privacy by design;
- furnishing of information and access to data subjects of their personal data;
- imposition of security safeguards for personal data;
- reporting of personal data breaches;
- maintenance of records relating to processing activities;
- carrying out of data protection impact assessments, and;
- appointment of data protection officers for monitoring and compliance.

4.2 Privacy by design

Privacy by design focuses on ensuring privacy and data protection rights from the “design phase of any system, service, product or process and then throughout its lifecycle.”²⁵⁴ Instead of thinking about privacy as an afterthought, privacy by design calls for proactively embedding good privacy practices into the design and operation of systems, infrastructure, and business practices, as explored in Fig. 4.1 below. Privacy by design strategies are useful to ensure privacy, generate trust, and secure data.²⁵⁵ The former Information and Privacy Commissioner of the Canadian Province of Ontario, defines privacy by design as generally consisting of seven foundational principles:²⁵⁶

- **Proactive and not reactive** – events risking privacy are anticipated and prevented before they occur;
- **Privacy by default** – privacy is built into the system by default and is not dependant on actions undertaken by data subjects;
- **Privacy embedded into design** – privacy is a core feature and is integrated into operations, technologies, and information systems rather than being thought of as an add-on;
- **Full functionality** – privacy by design aims to satisfy all legitimate objectives and not pit privacy against other objectives such as security. Privacy is to be embedded in a

254 ‘Data Protection by Design and Default’ (UK Information Commissioner’s Office) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>.

255 Farida H. Semantha, Sami Azam, Kheng Cher Yeo and Bharanidharan Shanmugam, ‘A Systematic Literature Review on Privacy by Design in the Healthcare Sector, (2020) 9(3) Electronics 452, 453.

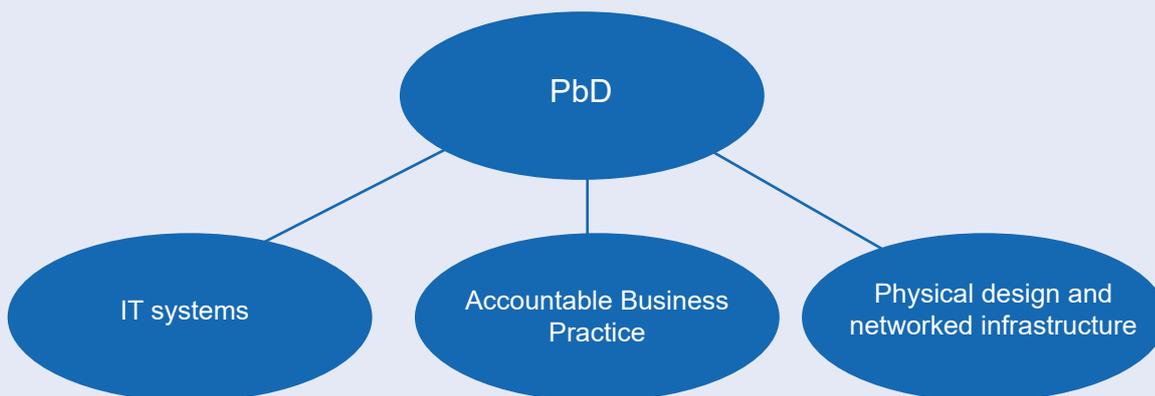
256 Ann Cavoukian, ‘Privacy by Design - The 7 Foundational Principles’ (2011) <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

technology, process, or system in a way that does not impair its full functionality while also ensuring security;

- End-to-end security over the entire lifecycle – privacy, once embedded into the system, extends throughout the data lifecycle and serves to foster accountability and data security;
- Visibility and transparency – to ensure accountability and increase trust, component parts and operations are open and transparent, and stakeholders are assured that all business practices and technologies are operating as per stated promises and objectives;
- User-centricity – design and operation of systems should be designed around the interest and needs of individuals, through measures such as maintaining privacy as the default mode.

The application of the principles described above can be exemplified in the design and operation of a typical web page that automatically collects information from users. In this case, privacy by design can require that the user interface is laid out in such a way that users are proactively informed of the web page’s cookie usage and are given a clear option to accept or refuse them. It would require that consent for such data collection is not based on pre-checked box forms. Rather, they require active consent, which requires that users be able to check the box form themselves. Such models could, however, lead to issues such as consent fatigue (as discussed in Chapter 3 on Data Protection Principles). Privacy by design also involves designing the collection and storage process in such a way that only strictly necessary information is collected. It also involves promoting the ability to unlink the identifiability of an individual from their personal data through measures, such as pseudonymisation.

Fig 4.1: The Privacy by Design Trilogy



PbD as a concept applies to a trilogy of encompassing applications.²⁵⁷

257 Ann Cavoukian, 'Privacy by Design - The 7 Foundational Principles' (2011) <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

4.2.1 Existence of requirement to institute privacy by design

Not all the Identified Regional Frameworks have incorporated privacy by design as a concept that requires data controllers and processors to build their systems around the principle of individual privacy. Among the frameworks, privacy by design principles are acknowledged only in Convention 108+, the OECD Guidelines, the APEC Privacy Framework, the GDPR, and the OAS Principles.

4.2.2 Content of privacy by design requirements

Article 10(2) of Convention 108+ requires data controllers and processors to “examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects” before they commence such processing. It also states that data processing should be designed to “prevent or minimise the risk of interference with those rights and fundamental freedoms.”

The OECD Guidelines have provisions that are relevant to privacy by design under data controller obligations on implementing accountability. They require data controllers to have in place a privacy management programme that not only gives effect to the OECD Guidelines for all personal data under their control, but is tailored to their processing operations (structure, scale, volume, and sensitivity), and provides for appropriate security safeguards. The programme must also be integrated into their governance structures with internal oversight mechanisms. It must include plans for responding to inquiries and incidents, and must be periodically reviewed and updated. The data controller is also required to “demonstrate its privacy management programme” at the request of a competent privacy enforcement authority.²⁵⁸

The APEC Privacy Framework prescribes that personal information protection should be “designed to prevent the misuse of [personal] information”. It

also calls for specific obligations which take into account the risk of harm that may result from misuse of such information, and taking remedial measures which should be “proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information”.²⁵⁹

The GDPR has specific provisions dealing with data protection by design and default. Article 25(1) prescribes that data controllers shall implement “appropriate technical and organisational measures, such as pseudonymisation” that are “designed to implement data protection principles, such as data minimisation” in an effective manner and to integrate the necessary safeguards into the processing. These measures will be implemented both “at the time of the determination of the means of processing and at the time of the processing itself.” The measures will be implemented “taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.”

The GDPR also adopts the principle of data protection by default. Recital 78 requires technical and organisational measures to be accounted for at the time of planning a processing system to protect data safety. Article 25(2) requires that data controllers implement the appropriate technical and organisational measures such that by default, only personal data which is necessary for each specific purpose is processed. The GDPR also specifies that this obligation applies to the amount of personal data collected, the extent of processing, the period of storage, and its accessibility. Such technical and organisational measures would ensure that that by default the personal data will not be made accessible without the relevant individual’s intervention “to an indefinite number of natural persons.”²⁶⁰ Importantly, Article 25(3) also indicates that compliance with requirements relating to technical and organisational measures can be demonstrated through approved certification mechanisms under Article 42 of the GDPR.²⁶¹

258 OECD Guidelines, Chapter 1, Part 3, para 15(a,b).

259 APEC Privacy Framework, Part iii, para 20. These obligations include measures such as: (i) self-regulatory efforts; (ii) education and awareness campaigns; and (iii) laws, regulations, and enforcement mechanisms.

260 GDPR, art 25(2).

261 Certification mechanisms (and data protection seals or marks) would also enhance transparency and enable data subjects to assess the data protection levels of products and services. See GDPR, recital 100.

The GDPR also leaves the adoption of specific measures to implement privacy by design open to legislation. Recital 78 gives the example of pseudonymisation, which involves de-identification of personal data through the use of artificial identifiers (as discussed in Chapter 2 on Key Definitions).

The OAS Principles note that privacy by design is a form of proactive accountability and relates to processor and controller actions before they even collect or begin to process data. It requires privacy and security considerations to be incorporated into every stage of product design. Data processing should also prioritise user privacy and data protection. It also notes that privacy by default requires personal data to be treated proportionally to the purpose for which it was collected, and that privacy by default should be “completely implemented” prior to data processing. It specifies that special care should be taken to reinforce the protection of sensitive data when operationalising privacy by design and default, that risks be identified and measures be taken to mitigate them based on requirements under domestic law.²⁶²

More generally, the OAS principle of accountability requires controllers to establish and comply with data protection goals. However, data controllers can be permitted to determine the most appropriate ways to reach those goals and monitor compliance in a manner that best serves their business models and customers. They note that controllers should be able to implement appropriate technical and organisational measures to demonstrate compliance with data protection principles. Processors should also be required to provide sufficient guarantees to ensure the protection of a data subject’s rights. Codes of conduct or certification mechanisms may be used to demonstrate compliance. National regulatory frameworks should provide guidance for data controllers, especially to demonstrate accountability.²⁶³

Privacy by design forms a core component of data protection. Requiring both public and private data controllers and processors to institute such programmes can significantly contribute to the protection of individuals’ privacy. It also helps create

accountability measures and safeguards to address the risks of large-scale data collection and use, such as exclusions, discrimination, and surveillance. It is especially important for data controllers and processors to adhere to, and demonstrate compliance with, objective standards of data protection when the use and collection of personal data is linked to the provision of essential services. Technical guarantees that support privacy laws and regulations, as well as the protections provided therein, are essential to meaningfully enforce data protection obligations.²⁶⁴

“Requiring both public and private data controllers and processors to institute such programmes can significantly contribute to the protection of individuals’ privacy.”

262 OAS Principles with Annotations, Principle 10, p 22-23.

263 OAS Principles with Annotations, Principle 10, p 22.

264 Prashant Agrawal, Anubhuti Singh, Malavika Raghavan, Subodh Sharma and Subhashis Banerjee, An operational architecture for privacy-by-design in public service applications, December 2020, 5. available at <https://www.dvara.com/research/wp-content/uploads/2020/12/An-operational-architecture-for-privacy-by-design-in-public-service-applications.pdf>.

Box 4.1: Privacy Enhancing Technologies

According to the European Commission, privacy enhancing technologies, or PETs, are defined as “a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system”.²⁶⁵ Using PETs is an important way to implement privacy by design. Well known PETs include pseudonymisation, encryption and obfuscation.²⁶⁶

Box 4.2: Privacy by Design Application Areas

Ontario’s former Information and Privacy Commissioner, who coined the term ‘privacy by design’, has identified nine application areas that directly relate to privacy by design:²⁶⁷

- CCTV/surveillance cameras in mass transit systems
- Biometrics used in casinos and gaming facilities
- Smart meters and the smart grid
- Mobile devices and communications
- Near field communications (NFC)
- RFIDs and sensor technologies
- Redesigning IP geolocation data
- Remote home health care
- Big data and data analytics.

265 Commission of the European Communities, ‘Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)’ COM (2007) 228 final.

266 European Union Agency for Network and Information Security, ‘Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics’, December 2015, Chapter 4, available at <https://arxiv.org/abs/1512.06000>; Zbigniew Kwecka and others, “I am Spartacus”: privacy enhancing technologies, collaborative obfuscation and privacy as a public good’ (2014) 22/2 Artificial Intelligence and Law pp 114-115 <https://www.research.ed.ac.uk/en/publications/i-am-spartacus-privacy-enhancing-technologies-collaborative-obfus>.

267 Ann Cavoukian, ‘Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices’ (Information and Privacy Commission, Ontario, December 2012), pp 55-58 <https://collections.ola.org/mon/26012/320221.pdf>.

4.3 Information and access to personal data

Transparency is a key requirement of privacy and data protection law. In data protection law, transparency engenders trust in citizens about data processing activities by enabling them to understand and challenge those activities. It is an expression of the data protection principle of “lawfulness and fairness”. When duly complied with, transparency requirements empower data subjects to exercise control over their personal information, for instance by withdrawing consent, or by holding controllers and processors accountable. Transparency obligations on controllers are complemented by the right of data subjects to access their personal data and related information.²⁶⁸

Data protection law usually aims to achieve transparency in data processing by requiring controllers and processors to implement a series of practical measures to provide information to data subjects regarding their data processing and management practices. Emphasis is also placed on the quality, accessibility and comprehensibility of the information provided to data subjects.²⁶⁹

4.3.1 Existence of requirement to provide information and access

All the Identified Regional Frameworks have incorporated provisions that specifically enshrine and promote transparency by data controllers.

4.3.2 Content of information to be provided

All the Identified Regional Frameworks require data controllers to provide information to data subjects regarding the processing of their data. Generally, this information includes:

- the fact that personal data is being collected;
- the data controller’s identity and address;
- the legal basis and the purposes of the intended processing;
- the categories of personal data processed;
- the recipients or categories of recipients of the personal data, if any;
- the means by which data subjects can exercise rights such as the right to access, correct and rectify personal data.²⁷⁰

The GDPR requires more information to be provided. It requires providing information, such as the controller’s intention to transfer personal data to third countries or international organisations.²⁷¹ Where applicable, the existence of adequacy decisions by the European Commission and suitable safeguards in such cases are also to be mentioned. Other information must also be provided, such as the fact that data subjects have the right to lodge a complaint with the national supervisory authority, whether the provision of data by the data subject to the controller is based on a statutory or a contractual requirement, and the existence of any automated decision-making, specifically including profiling.²⁷²

268 Art. 29 Working Party, Guidelines on Transparency under Regulation 2016/679 of 29 November 2017 by the working party on the protection of individuals with regard to the processing of personal data [2017] WP260 rev.01 (as revised and adopted on 11 April 2018), pp 4-5.

269 Art. 29 Working Party, Guidelines on Transparency under Regulation 2016/679 of 29 November 2017 by the working party on the protection of individuals with regard to the processing of personal data [2017] WP260 rev.01 (as revised and adopted on 11 April 2018), p 5.

270 Convention 108+, art 8; OECD Guidelines, paragraph 12, and paragraph 12, OECD Guidelines, Original Explanatory Memorandum, Chapters 1 and 3, OECD Guidelines; Commonwealth PPI Bill, s 21(5); Commonwealth Model Privacy Bill, s 8(2); APEC Privacy Framework, Part iii, para 21; AU Convention, art 16; ASEAN DP Framework, para 6(a); OAS Principles with Annotations, principle 2; HIPCAR Model Legislative Text, s 10; GDPR, arts 12-14.

271 GDPR, art 13(1)(f).

272 GDPR, art 13(2).

The GDPR and Convention 108+ provide exceptions when it is not necessary to provide this information, namely when the data subject already has the information or when it proves impossible or involves disproportionate efforts because the data subject is not clearly identifiable or the controller has no way of contacting the data subject.²⁷³ The APEC Privacy Framework exempts situations, such as the collection of publicly available information and business contact information.²⁷⁴ However, the AU Convention, OAS Principles, OECD Guidelines, HIPCAR Privacy Framework and the Commonwealth PPI and Privacy Bills do not permit specific exceptions to this requirement. The ASEAN DP Framework simply provides that controllers may collect, use or disclose personal data without notification to or consent of the data subject, when such actions are authorised or required under domestic laws.²⁷⁵ Public bodies and government agencies are not specifically exempted from this transparency requirement under the Identified Regional Frameworks. The obligation placed on controllers to provide information is complemented by the data subjects' right to access information. This right, and applicable exemptions are discussed in Chapter 5 (Rights of Data Subjects).

4.3.3 *When to provide this information*

In most of the frameworks, this information is to be provided at the time of collection. When this is not possible it should be provided as soon as reasonably possible following collection. For instance, the OAS Principles require that the legal basis for processing, the data processing purposes and other information must, as a rule, be specified at or before the time of data collection. The practices and policies of the entities collecting data must also be provided so that the data subjects are able to make informed decisions whether to give the relevant information.²⁷⁶ The GDPR not only requires information to be provided when the data is collected, but at all stages of processing under Article 12.



273 GDPR, arts 13(4) and 14(5); Convention 108+, art 8(2) and 8(3).

274 APEC Privacy Framework, Part iii, paras 21-23.

275 ASEAN DP Framework, Para 6(a)(ii).

276 OAS Principles with Annotations, Principle 2, p 9.

Box 4.3: Transparency under the GDPR

As the Article 29 Data Protection Working Party's Guidelines on Transparency state, transparency under the GDPR should be applied at all stages of the data processing lifecycle:

- before or at the start of the data processing cycle (i.e., at the time when the personal data is being collected, either from the data subject or otherwise obtained);
- throughout the whole processing period (i.e., when communicating with data subjects about their rights); and
- at specific points while processing is ongoing (e.g., when data breaches occur or in the case of material changes to the processing).²⁷⁷



²⁷⁷ Art. 29 Working Party, Guidelines on Transparency under Regulation 2016/679 of 29 November 2017 by the working party on the protection of individuals with regard to the processing of personal data [2017] WP260 rev.01 p 6.

4.3.4 How to provide the information

Mandating that data controllers are required to provide the information discussed above to data subjects is not sufficient. The requirement that the information should also be easily understandable, accessible, and conveyed through clear and plain language is common across the frameworks. This is to enable the average person to understand the information provided by data controllers so that as a data subject, they can make meaningful choices with respect to the use of their data. Although children can also be data subjects, specific provisions relating to these categories of data subjects are found only in the GDPR and the OAS Principles. They highlight that information provided to children should be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.²⁷⁸ Data controllers can also be required to provide information in alternative formats to those with disabilities pursuant to the right of data subjects to access information,²⁷⁹ as noted in Chapter 5 (Rights of Data Subjects).

4.3.4.1 Transparency in government processing

Transparency provisions are essential for public authorities and government agencies. The ECJ has ruled that the transfer of personal tax data by one Romanian public authority to another for processing, without first informing the data subjects, violated the fair processing requirement.²⁸⁰ This decision was rendered on the basis of the Data Protection Directive.²⁸¹

Transparency in government processing is important since governments collect large amounts of personal data for various purposes, such as for identity documents, state bank records, and evidence gathering by law enforcement. The need for limits on governmental use of personal data has become critical in light of the large-scale collection of personal data during the COVID-19 pandemic. Much of this data collection, such as contact tracing through many methods, such as geospatial tagging and flow modelling, was conducted in the absence of enabling laws or regulations governing data-sharing. Sensitive health data collected during this time is at heightened risk in jurisdictions without data protection laws. Some countries have reportedly shared such contact-tracing data with law enforcement,²⁸² or have used intelligence software originally intended to track terrorist activity for contact-tracing efforts.²⁸³

278 GDPR, art 12(1); OAS Principles with Annotations, Principle 2, p 9.

279 Commonwealth PPI Bill, s 26; HIPCAR Model Legislative Text, s26(2); OAS Principles with Annotations, Principle 8, p 18.

280 Case C-201/14 Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others [2015] pp 34-35, 38, 41, 46.

281 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (repealed as on 25 May 2018).

282 BBC News, Andreas Illmer, 'Singapore reveals Covid privacy data available to police', 5 January 2021 <https://www.bbc.com/news/world-asia-55541001>.

283 The Indian Express, 'Covid-19: Pakistan uses militant-tracking technology for contact tracing', 28 May 2020 <https://indianexpress.com/article/pakistan/pakistan-surveillance-technology-militants-coronavirus-6431271/>; Moran Amit and others, 'Mass-surveillance technologies to fight coronavirus spread: the case of Israel' (2020) *Nat Med* 26, 1167–1169 <https://doi.org/10.1038/s41591-020-0927-z>

4.4 Security safeguards

Across the world, security threats to personal information are on the rise. The average number of cyberattacks and data breaches increased 15% in 2021 from the previous year, and are set to rise further.²⁸⁴ By imposing mandatory data security measures, data protection laws can serve to mitigate the adverse effects of data and cybersecurity threats.²⁸⁵

Data security involves processing data securely by means of certain technical and organisational measures. Technical measures include both physical measures, such as quality of doors and locks, CCTV and disposal policies, as well as ICT security, which includes security of network and information systems, online security, authorisation and authentication policies and device security, among others.²⁸⁶

Legal provisions requiring data security measures seek to prevent privacy violations. Their objective is to protect the “confidentiality, integrity and availability” of personal data to ensure: (i) that only those authorised to do so can access, alter, delete, or disclose data within the limits of their authority; (ii) the accuracy and completeness of data; and (iii) the accessibility, usability and recoverability of personal data.²⁸⁷

4.4.1 Existence of requirement to provide security safeguards

Data security is broadly recognized as a basic principle of data protection across all Identified Regional Frameworks. All frameworks have provisions requiring data controllers and processors to ensure

data security.

4.4.2 Level of data security prescribed

Since data security involves the imposition of measures that can be quite varied and complex, the standard commonly employed in the Identified Regional Frameworks is that of “appropriate(ness)” or “reasonable(ness)” to ensure that the measures to be used for ensuring data security are required to be “appropriate” or “reasonable.”²⁸⁸ Although data security is a mandatory requirement across all Identified Regional Frameworks, the specific measures to be implemented are often left to national regulators or supervisory authorities to develop later, and authorities should take into account different factors such as the sector, kind of controller or processor, and the nature of data. The obligation to ensure data security focuses more on the conduct of controllers and processors rather than on the outcome of processing.

4.4.3 A risk-based approach

Relatedly, the frameworks also acknowledge that the safeguards can vary depending on several factors and emphasize that the security safeguards should be proportional to the risk of harm. The APEC Privacy Framework provides that safeguards should be “proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held.”²⁸⁹ The GDPR states that factors such as “the state of the art, the costs of implementation and the nature, scope, context

284 'Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know' (Forbes) <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/>.

285 Gloria González Fuster and Lina Jasmontaite 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds) *The Ethics of Cybersecurity* (Springer 2020).

286 UK Information Commissioner's Office, 'Guidance on Data Security: Guide to the General Data Protection Regulation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/#6>.

287 Ibid.

288 GDPR, art 5(1)(f); ASEAN DP Framework, para 6(d); APEC Privacy Framework, Part iii, para 28; HIPCAR Model Legislative Text, s 14(1); OAS Principles with Annotations, principle 6, p 15; Commonwealth Model Privacy Bill, s 18(1).

289 APEC Privacy Framework, Part iii, para 28.

and purposes of processing,” and the likelihood and severity of risks to the rights and freedoms of natural persons, will determine the security safeguards to be employed.²⁹⁰

The OAS Principles note that the measures adopted to protect personal data can depend on the effects on data subjects’ rights, implementation costs, the nature of data and purposes of processing, and the sensitivity of the relevant data.²⁹¹ They also specify that the principle of security is not necessarily violated by data controllers in case of unauthorised access, destruction, and other such consequences as long as the safeguards implemented were “reasonable and appropriate.”

The determination of what is reasonable and appropriate would be based on best-practice and other factors, such as the proportionality and necessity of measures taken and the evolution of privacy threats. The Principles require the measures undertaken to be subject to “periodic review, reassessment, audit, updating and improvement”. They also specify that protecting the privacy of data subjects requires that they have control over their online experience, and that controllers should “have the flexibility” to provide users with tools to effectively control data sharing.²⁹² They also state that controllers should be responsible for ensuring that any third parties who receive personal data from them comply with applicable safeguards and requirements.²⁹³

Box 4.4: Obligation of Conduct, Not Result

The obligation to put in place security safeguards to protect personal data generally appears to focus on the conduct of controllers and processors and not on the result, such as a breach of personal data. For instance, a 2015 hack leaked personal data from the popular e-Bay internet auction website in South Korea. The country’s Supreme Court upheld the lower court’s ruling that eBay had not violated its obligations under the Standards for Technical and Administrative Protective Measures for Personal Information established by the Ministry of Information and Communication, since it had taken all reasonable and necessary measures to protect personal information.²⁹⁴ The Supreme Court took into context the hacking methods used, the level of security technology available at the time, and the overall security measures taken by eBay.

290 GDPR, art 32(1).

291 OAS Principles with Annotations, Principle 6, p 15.

292 OAS Principles with Annotations, Principle 6, p 15.

293 OAS Principles with Annotations, Principle 10, p 23.

294 Supreme Court Decision 2013Da43994, 44003, decided February 12, 2015 <https://library.scourt.go.kr/SCLIB_data/decision/06-2013Da43994.htm> accessed 31 October 2021.

4.4.4 Harms to be protected against

A study of the Identified Regional Frameworks indicates that the typical harmful consequences that data security measures seek to prevent include accidental or unlawful destruction, loss, alteration, and unauthorised disclosure or access to personal data.²⁹⁵ The ASEAN DP Framework, Commonwealth PPI Bill, and the APEC Privacy Framework also include copying, modification, destruction, and similar risks.²⁹⁶

4.4.5 Processing on behalf of the controller and third-party processing

Data protection legislations also require compliance with data security measures in cases where processing is undertaken on behalf of the controller or by a third party. For instance, the Commonwealth PPI Bill holds an organisation responsible for personal information in its custody or control, including information that has been transferred to a third-party for processing.²⁹⁷ The AU Convention provides that “where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees,” and that it is “incumbent on the controller and the processor to ensure compliance with the security measures defined in [the] Convention.”²⁹⁸ The HIPCAR Privacy Framework also requires the controller to ensure that the person processing personal information on its behalf “can implement the security measures that must be taken” and “actually takes the measures so identified.”²⁹⁹

In a related provision, Section 33 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 (implementing the Philippines’ Data Privacy Act, 2012) contains additional obligations for private service providers acting on behalf of government agencies. Where the government enters into contracts with

service providers, such that they may be required to access the sensitive personal information of more than 1000 individuals, government agencies must require the service providers to register their data processing systems with the supervisory authority. They are also required to comply with other obligations under the Act that are applicable to government agencies and their employees.

From a transparency point of view, the security safeguards or data security measures taken by the controllers and processors can also be one of the details that should be disclosed to data subjects, as required in the Commonwealth PPI Bill.³⁰⁰ Furthermore, the GDPR provides that certification mechanisms or adherence to codes of conduct can demonstrate compliance with security requirements.³⁰¹ Periodic review of the security measures taken is also a requirement of data protection law, as evidenced by the OAS Principles and the GDPR.³⁰²

The legal requirement to establish security safeguards is complementary to more specific obligations, such as data breach notifications, data minimisation, and data quality.³⁰³ Notably, provisions pertaining to data security are more commonly framed as obligations on data controllers and processors, and not as rights to be exercised by data subjects. Commentators have pointed out that it may be useful to also include them as data subjects’ rights and to empower them with remedies against data controllers.³⁰⁴

295 GDPR, art 32(2).

296 ASEAN DP Framework, para 6(d); s 18(1), Commonwealth PPI Bill; APEC Privacy Framework, Part iii, para 28.

297 Commonwealth PPI Bill, s 18(2).

298 AU Convention, principle 6, art 13.

299 HIPCAR Model Legislative Text, s 14(2).

300 Commonwealth PPI Bill, s 18(4).

301 GDPR, art 32(3).

302 OAS Principles with Annotations, Principle 6, p 15; GDPR, art 32(1)(d).

303 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ (2018), 66.

304 Dvara Research, ‘Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019’ (2020) p 4 <https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf>.

Box 4.5: Illustrations of the Cost of Data Security Breaches

- In March 2020, SolarWind, a third-party vendor to several US government agencies and Fortune 500 companies, was hacked through a software update that it had sent to its clients. Discovered in December 2020, the breach is one of the biggest in history, with the breach costing the company at least \$18 million in the first quarter of 2021.³⁰⁵ The full scale of the breach is still being investigated.³⁰⁶
- In March 2017, the failure to patch a well-known vulnerability at Equifax, a US credit rating agency, resulted in a security breach that disclosed the personal data and sensitive financial data of hundreds of millions of people in the United States. The settlement is expected to cost Equifax at least \$650 million.³⁰⁷
- In 2014, a data breach at Marriott International resulted in the personal data (including credit and debit card details) of 383 million guests being leaked, putting them at risk of identity theft and social-engineering frauds.³⁰⁸

305 Reuters, Raphael Satter, 'SolarWinds says dealing with hack fallout cost at least \$18 million', 14 April 2021 <https://www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/>.

306 'SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president' (Reuters, 15 February 2021) <https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R>.

307 Stacy Cowley, 'Equifax to Pay at Least \$650 Million in Largest-Ever Data Breach Settlement', The New York Times (2019) <https://www.nytimes.com/2019/07/22/business/equifax-settlement.html>; Neil Daswani and Moudy Elbayadi, Big Breaches: Cybersecurity Lessons for Everyone (Springer 2021), ch 4.

308 Neil Daswani and Moudy Elbayadi, Big Breaches: Cybersecurity Lessons for Everyone (Springer 2021), ch 3.

4.5 Reporting of personal data breach

The breach notification requirements in data protection laws typically oblige entities that control and process data to notify a supervisory authority and/or affected data subjects if there has been unauthorised access to data.³⁰⁹ The objective of notifications is to enable the affected data subjects to take steps to mitigate the risks to their data, as well as to incentivise entities to implement and strengthen their data security measures.³¹⁰

4.5.1 Existence of breach notification requirements

Among the Identified Regional Frameworks, Convention 108+, the OECD Guidelines, the GDPR and the OAS Principles have mandatory notification requirements if a personal data breach takes place. Meanwhile the Commonwealth PPI and Privacy Bills, the AU Convention, ASEAN DP Framework and the HIPCAR Privacy Framework do not. The APEC Privacy Framework notes that requiring that the data protection authority and/or data subjects are notified of breaches can reduce the risk of harm to the relevant individuals, and notes that Member States should “consider encouraging or requiring personal information controllers to provide notice” in case of significant data security breaches.³¹¹

4.5.2 Defining a personal data breach

Among the Convention 108+, the OECD Guidelines, the GDPR and the OAS Principles (that have the mandatory data breach disclosure requirements), only the GDPR defines what constitutes a personal data breach. Defining a personal data breach adds clarity on notification requirements, and reduces the possibility of confusion or lack of clarity among controllers, processors and supervisory authorities as to when to notify and when to not.³¹² A personal data breach in the GDPR is defined as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”³¹³

4.5.3 Threshold requirements for personal data breach notifications

Convention 108+, OECD Guidelines, and GDPR require minimum thresholds to trigger the notification requirement. Convention 108+ requires notifications of data breaches which may “seriously interfere with the rights and fundamental freedoms of data subjects”.³¹⁴ Instances that qualify as serious interference are provided by the Explanatory Report to Convention 108+, which include “disclosure of data covered by professional confidentiality, or which may result in financial, reputational, or physical harm or humiliation”.³¹⁵

309 Ravi Sen and Sharad Borle, ‘Estimating the Contextual Risk of Data Breach: An Empirical Approach’ (2015) 32(2) *Journal of Management Information Systems* 314.

310 See ‘Security Breach Notification Laws: Views from Chief Security Officers’ (December 2007) Samuelson Law, Technology and Public Policy Clinic, University of California-Berkeley School of Law, available at https://www.law.berkeley.edu/files/cso_study.pdf.

311 APEC Privacy Framework, Part iii, para 20 and Part iv, para 54.

312 Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, Faiza Rahman, ‘Comments on the (Draft) Personal Data Protection Bill, 2018’ (2018) NIPFP, 13 <https://www.medianama.com/wp-content/uploads/NIPFP-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>.

313 GDPR, art 4(12).

314 Convention 108+, art 7(2).

315 Explanatory Report to the Convention 108+, p 22, para 64. The text of the Explanatory Report to the Convention 108+ is intended to guide and assist the application of the provisions of the Convention and provides an indication as to how the drafters envisaged the operation of the Convention.

The OECD Guidelines require notification to supervisory authorities when a “significant security breach affecting personal data” takes place and to data subjects when “the breach is likely to adversely affect” them.³¹⁶

Similarly, the GDPR requires notification to the supervisory authority only when the breach is likely to result in a “risk to the rights and freedoms of natural persons,” while notifications to the data subjects are required when the “personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.”³¹⁷ The OAS Principles note that controllers should notify data subjects and relevant authorities in some cases, but do not specify thresholds. They also note that reporting requirements are imposed by relevant domestic law by member states.³¹⁸

Who data controllers are required to notify in case of personal data breaches

Convention 108+ requires notifying only the supervisory authority mandatorily.³¹⁹ However, its Explanatory Report recognises that the controllers may need to notify data subjects in other situations, for example when the breach is likely to result in a significant risk for the rights and freedoms of individuals (e.g., discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage).³²⁰

The OECD Guidelines and the GDPR require notifications to both supervisory authorities and data subjects on meeting their respective threshold, as explained above.³²¹

The OAS Principles require data controllers to notify relevant data subjects in the event of a breach, and to also inform relevant criminal or civil authorities. They note that notification laws may also require controllers to cooperate with other agencies (e.g.

entities responsible for cybersecurity). Breach notification laws may, in limited and specific situations, impose obligations on controllers to cooperate with law enforcement agencies and share personal data without the consent of the relevant data individuals. However, the OAS Principles require that states are careful to not impose conflicting notification and confidentiality obligations on controllers.³²²

“The objective of (breach) notifications is to enable the affected data subjects to take steps to mitigate the risks to their data, as well as to incentivise entities to implement and strengthen their data security measures”

316 OECD Guidelines, Chapter 1, Part 3, para 15(c).

317 GDPR, arts 33(1) and 34(1).

318 OAS Principles with Annotations, Principle 6, p 16.

319 art 7(2), COE 108+.

320 Explanatory Report to the Convention 108+, paras 64-66, pp 22-23.

321 OECD Guidelines, Chapter 1, Part 3, para 15(c); GDPR, arts 33(1) and 34(1).

322 OAS Principles with Annotations, Principle 6, p 16.

Box 4.6: Breach Notification Database

Some experts have noted the utility of making breach notifications public, either on the website of the supervisory authority,³²³ or in a centralised database.³²⁴ This would not only incentivise organisations to improve security for fear of reputational loss, but also make available data for research and assist enforcement agencies without compromising security incentives.

4.5.5 Applicability of notification obligations for personal data breaches

By and large, the frameworks place the obligation to notify data breaches on data controllers. The GDPR applies it specifically to processors and requires them to notify all personal data breaches to controllers, regardless of thresholds. They are required to do so without delay after becoming aware of the breach.³²⁵ It then falls to the controllers to notify the supervisory authorities and/or the data subjects, depending on whether the personal data breach meets the threshold requirements. Commentators have pointed out that since processors under the GDPR also have the responsibility for ensuring data security,³²⁶ it is arbitrary to not require the processor to directly report breaches to supervisory authorities or data subjects, especially since security breaches can take place at many different levels including at the processor level.³²⁷

While none of the Identified Regional Frameworks distinguish between government and private data controllers with respect to breach notification requirements, they do envisage exemptions to this provision, typically on the grounds of national security, public safety, public order and investigation and prosecution of criminal offences for government entities.³²⁸ Notably, the GDPR does not exempt compliance with this provision on these grounds.

Providing exemptions from such requirements, especially for a broad range of purposes, can significantly impair the ability of data subjects impacted by a breach to exercise their rights under data protection law, and to take the necessary measures to mitigate the effects of the breach.

323 Angela Daly, 'The introduction of data breach notification legislation in Australia: A comparative view, Computer Law & Security Review' (2018) Computer Law & Security Review 16.

324 'Security Breach Notification Laws: Views from Chief Security Officers' (December 2007) Samuelson Law, Technology and Public Policy Clinic, University of California-Berkeley School of Law, p 13, available at https://www.law.berkeley.edu/files/cso_study.pdf.

325 GDPR, art 33.

326 GDPR, art 30(2)(d).

327 P Blume, 'Controller and Processor: Is There a Risk of Confusion?' (2013) 3 IDPL 140, 144.

328 Convention 108+, art 11; para 4, OECD Guidelines, Chapter 1.

Box 4.7: Breach notification requirements

A study by the Samuelson Law, Technology and Public Policy Clinic, University of California Berkeley School of Law, which examined the views of several Chief Security Officers in major organisations, found that:³²⁹

- Breach notification requirements are directly related to companies increasing and improving their data security measures to avoid reputational loss and to avoid seeming irresponsible.
- They raise awareness levels within organisations and increase cooperation among different departments within organisations.
- As organisations are made responsible for data breaches, they exert pressure on other organisations holding data to meet data security standards, improving overall industry standards through flow-on effects.



329 'Security Breach Notification Laws: Views from Chief Security Officers' (December 2007) Samuelson Law, Technology and Public Policy Clinic, University of California-Berkeley School of Law, available at https://www.law.berkeley.edu/files/cso_study.pdf.

4.6 Maintenance of records relating to processing activities

Maintaining records is an organisational requirement and a measure of good data governance.³³⁰ As an element of the accountability principle, it helps supervisory authorities monitor organisations to show compliance with data protection laws. Organisations are ordinarily required to keep a record of their processing activities, including processing purposes, data retention and sharing activities. Among other areas, records pertaining to categories of data subjects and personal data, transfers to third parties and their practices, and use and processing of personal data without consent are also included.

4.6.1 Existence of record maintenance requirements

The GDPR and the Commonwealth PPI Bill are the only regional frameworks that recognise and impose record maintenance requirements as distinct from data retention obligations.

4.6.2 Form and content of records to be maintained

The Commonwealth PPI Bill requires an organisation to record of “all uses and disclosures that it makes of personal information about an individual” without consent.³³¹ Organisations are also required to note personal information about the individual that they have in their custody or control, either as part of the records of such personal information or in a form linked to those records.³³²

The GDPR requires the maintenance of far more detailed records. It requires controllers to maintain a record of processing activities. Meanwhile, processors must maintain records of all categories of processing

activities carried out on behalf of a controller. Such records must be “in writing, including in electronic form” and must be made available to the supervisory authority if so requested.³³³

The GDPR also specifies the details that need to be contained in such records, which include the name and contact details of the controller and its data protection officer, the purposes of and legal basis for processing, categories of personal data and data subjects, the use of profiling, categories of cross-border transfers and a general description of the technical and organisational security measures.³³⁴ There are similar obligations placed on processors. The obligation to maintain records of processing activities can increase costs for data controllers and processors. However, they also provide increased accountability and provide necessary information in case of investigations of violations of data protection laws.

330 UK Information Commissioners Office, ‘Guide to the General Data Protection Regulation’ 1 January 2021, 171 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>.

331 Commonwealth PPI Bill, s 19(1).

332 Commonwealth Bill, s 19(2).

333 GDPR, art 30(1-4).

334 GDPR, art 30(1)(g).

Box 4.8: Data Retention versus Record Maintenance Obligations

Although the concepts appear to overlap, there is a distinction between data retention obligations and requirements to maintain records relating to processing. The former is concerned with the actual retention of personal data with obligations relating to the kinds of personal data to be preserved, the time periods for which they should be retained and their destruction post the specified periods. The latter is concerned with information on the processing of personal data and related practices, including the kind of processing activities by controllers and processors, the categories of data subjects and personal data, records of transfers to third parties and their practices, use and processing of personal data without consent, etc.

4.7 Data protection impact assessments

A data protection impact assessment (DPIA) is a process by which data protection risks are identified and managed and is a key measure through which privacy by design is implemented. The objective of a DPIA is to carry out a systematic assessment of data processing activities to highlight risks to data protection and to determine whether the processing is compliant with the law.³³⁵ This in turn allows organisations to take appropriate action to minimise those risks.³³⁶

DPIAs can be carried out for a system, database, programme, application, scheme or service, and even draft legislation.³³⁷ The scope, context and nature of processing are detailed in the DPIAs. It also involves making necessity and proportionality assessments, and considering the risks and harms posed to data

principals as well as action that can minimise the risks.³³⁸

4.7.1 Existence of DPIA requirements

Convention 108+, the OECD Guidelines, the GDPR, and the HIPCAR Privacy Framework require privacy or data protection impact assessments to be conducted, whereas the Commonwealth PPI and Privacy Bills, AU Convention and the ASEAN DP Framework do not. The APEC Privacy Framework notes the importance of “privacy management programmes” in ensuring accountability, and observes that Member States “should consider encouraging” data controllers to develop such programmes for all personal information under their control.³³⁹

335 Peter Carey, *Data Protection – A Practical Guide to UK and EU Law* (6th edn, OUP 2020) p 206.

336 Eduardo Ustaran (ed) *European Data Protection Law and Practice* (nd edn., IAPP 2019).

337 David Wright, ‘Should Privacy Impact Assessments be Mandatory?’ (2011) 54(8) *Communications of the ACM* 121, 124.

338 UK Information Commissioner’s Office, ‘Data Protection Impact Assessments’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.

339 APEC Privacy Framework, Part iii, para 32 and Part iv, paras 43-45.

Though the OAS Principles do not specifically provide for DPIAs, they note that privacy protection “depends upon a credible assessment of the risks” to data subjects and mitigation of such risks. They also state that appropriate resources should be provided for the implementation of data protection programmes, such as risk management systems and training and supervision.³⁴⁰

4.7.2 Threshold requirements for DPIAs

Among the frameworks, Convention 108+, the OECD Guidelines, and the HIPCAR Privacy Frameworks do not impose any thresholds for triggering DPIA requirements.³⁴¹ The HIPCAR Privacy Framework only requires public authorities to undertake privacy impact assessments. This is to be done “for any proposed enactment, system, project, programme or activity.”³⁴²

However, the GDPR requires a DPIA where processing, “in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing” is likely to result in a high risk to the rights and freedoms of individuals.³⁴³ It also specifically requires DPIAs in cases where: (i) the data processing involves an extensive evaluation of personal aspects, such as profiling; (ii) the processing involves special categories of data (such as revealing racial or ethnic origin), or data relating to criminal offences or convictions; or (iii) where the processing involves a systematic monitoring of a public space on a large scale.³⁴⁴

4.7.3 Procedure and content of DPIAs

Among the frameworks, only the GDPR and APEC Privacy Framework provide details on the procedure and content of DPIAs. According to the GDPR, the data controller must describe the proposed processing operation and the purpose being served by such operations. The DPIA must also reflect an assessment of the necessity and proportionality of the processing operation against its stated purpose. Lastly, it must contain an assessment of the possible risks to rights and freedoms of data subjects, and proposed security measures to address these risks and ensure compliance with the GDPR.³⁴⁵

The APEC Privacy Framework notes that privacy management programmes should: (i) be tailored to the structure and scale of operations of the relevant controller and the sensitivity of personal data that is being processed; (ii) provide appropriate safeguards based on the risk assessment; (iii) establish internal oversight and response mechanisms; (iv) be overseen by appropriately trained personnel; and (v) be monitored and regularly updated. It also requires data controllers be prepared to demonstrate their privacy management programmes at the request of the relevant data protection authority or other appropriate entity.³⁴⁶

4.7.4 Role of supervisory authority in DPIAs

None of the frameworks require approval for the DPIA from the supervisory authority. However, the GDPR allows Member States to make DPIAs mandatory when processing is required by the controller for the performance of a task which is in the public interest, such as for the purposes of social protection or public health.³⁴⁷

340 OAS Principles with Annotations, Principle 10, p 22.

341 Convention 108+, Art 10(2); Explanatory Report to the Convention 108+, p 25, para 88; para 15 OECD Guidelines, p 24 Supplementary Explanatory Memorandum to the OECD Guidelines, Chapters 1 and 2, OECD Privacy Framework; HIPCAR Model Legislative Text, s 28.

342 HIPCAR Model Legislative Text, s 28(1).

343 GDPR, art 35(1).

344 GDPR, art 35(3).

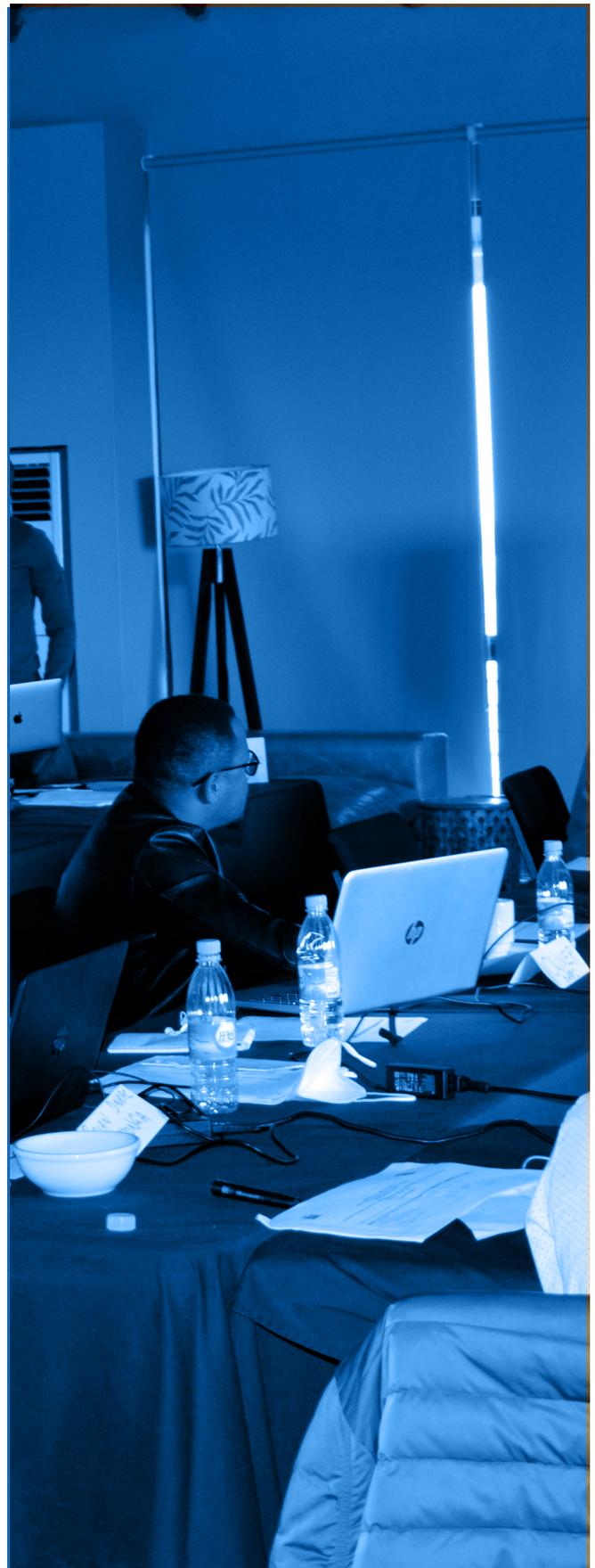
345 GDPR, arts 35(7)(a-d).

346 APEC Privacy Framework, Part iv, paras 44-45.

347 GDPR, art 36(5).d

The GDPR also provides the most scope for involvement from the supervisory authority. The supervisory authority is required to publish a list of processing activities that are subject to DPIAs and a list of processing activities that are not. The supervisory authority has to be consulted by the data controller when the processing will result in a high risk in the absence of mitigating measures.³⁴⁸ If the supervisory authority is of the opinion that the processing will infringe the GDPR, especially in cases where the risks have not been sufficiently mitigated or identified by the controller, the supervisory authority will provide written advice to the controller and the processor within eight weeks of receipt of the request for consultation.³⁴⁹ The supervisory authority is also enabled to issue warnings, reprimands, order compliance with the GDPR's provisions, as well as temporarily ban processing.³⁵⁰ The GDPR also lists the information to be provided by the controller to the supervisory authority, such as the respective responsibilities of the controllers and processors involved in the processing, the purposes of the intended processing, and the safeguards used to protect the rights and freedoms of data subjects. States must also consult supervisory authorities when proposals are prepared for legislative or regulatory measures relating to processing.³⁵¹

Mandating the use of DPIAs is central to implementing and designing effective privacy by design mechanisms. It can be tremendously useful in both public and private sector applications and forms part of data protection best practice. It can be especially important for the use of personal data by state agencies where vast amounts of personal data are collected and processed, and where the risks to data subjects can be the most significant, such as being excluded from public services or discrimination.



348 GDPR, art 36(1).

349 GDPR, art 36(2).

350 GDPR, art 58.

351 GDPR, art 36(3,4).

Box 4.9: Data Protection Impact Assessment Checklist

The UK Information Commissioner's Office has formulated a useful checklist for data controllers to carry out data protection impact assessments:³⁵²

- Describe the nature, scope, context and purposes of the processing;
- Ask data processors to help understand and document their processing activities and identify any associated risks;
- Consider the best way to consult relevant stakeholders (including data subjects);
- Ask for the advice of the data protection officer;
- Carry out necessity and proportionality assessments and describe how data protection principles will be complied with;
- Assess the likelihood and severity of risks to individuals' rights and interests;
- Identify measures that can reduce or eliminate high risks;
- Record decision-making with respect to the outcomes of the DPIA (including difference of opinions with DPOs);
- Review the DPIA and revisit, if necessary.

Box 4.10: Data Audits

Data audits are assessments of whether organisations are following good data practices. A data audit helps identify whether an organisation has effective controls, policies and procedures in place to comply with its data protection obligations. It typically involves identifying the different personal data an organisation collects, the sources for such data, the purposes for which it is collected, storage and retention practices and processing activities including third party transfers and the categories of third party recipients. The findings are then reviewed to determine whether the organisation is compliant with its data protection obligations, and if not, what needs to be done to make it compliant. The United Kingdom's Information Commissioner has published a [Guide to Data Audits](#) that can be referred to for further information.³⁵³

352 UK Information Commissioner's Office, 'Data Protection Impact Assessments' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.

353 UK Information Commissioner's Office, 'A Guide to ICO Audits' (2021) <<https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf>> accessed 31 October 2021.

4.8 Data protection officer

The Data Protection Officer (DPO) is an expert officer appointed by controllers to facilitate their compliance with data protection obligations, thereby ensuring transparency and accountability with data protection law. They play an important role in ensuring that controllers comply with data protection regulation. The DPO's functions ordinarily include compliance monitoring, developing procedures to demonstrate compliance and accountability, informing and advising on data protection obligations, as well as operating as a point of contact with both supervisory authorities and data subjects. DPOs are usually independent and report to the highest management, with several organisations often having a common DPO.³⁵⁴

4.8.1 Existence of requirement for DPOs

Convention 108+, OECD Guidelines, Commonwealth PPI Bill, the GDPR, the HIPCAR Privacy Framework and the OAS Principles envisage the appointment of a designated official by controllers to ensure data processing activities are compliant with data protection law.³⁵⁵ The APEC Privacy Framework, ASEAN DP Framework and AU Convention do not provide for such an official. In the HIPCAR Privacy Framework, this functional requirement is only required for the state due to the importance of effective oversight of data protection in public institutions.³⁵⁶ None of these frameworks have exempted public or governmental authorities from compliance with this requirement.

Box 4.11: DPOs under the GDPR

Under the GDPR, the controller and processor must appoint a DPO if:³⁵⁷

- they are a public body with the exception of courts acting in a judicial capacity;
- their core activities involve large scale processing requiring regular and systematic monitoring of data subjects, such as tracking and profiling, both online and offline, and;
- their core activities consist of large scale processing of special categories of data, such as genetic and biometric data, racial or ethnic data, or sexual orientation.

354 UK Information Commissioner's Office, 'Guide to Data Protection Officers' <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/>> accessed 31 October 2021.

355 Explanatory Report to Convention 108+, p 25, para 87; Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines, Chapter 2, p 24; Commonwealth PPI Bill, s 21(3); GDPR, arts 37-39; HIPCAR Model Legislative Text, s 31; OAS Principles with Annotations, Principle 10, p 22.

356 HIPCAR Model Legislative Text, s 31 and para 47, p 51.

357 GDPR, art 37.

4.8.2 Responsibilities of the DPO

Although phraseology of DPOs differs, the common responsibility of the DPO across frameworks is to demonstrate or ensure their controllers' compliance with applicable data protection law. According to the Supplementary Explanatory Memorandum to the Revised OECD Guidelines, they may play an important role in designing and implementing the privacy management programmes that controllers are required to have in place.³⁵⁸ The Commonwealth PPI Bill requires that they facilitate the organisation's compliance, ensure the organisation's employees are duly informed of their duties and respond to inquiries from the public about their information management practices.³⁵⁹ This requirement applies only to organisations in the private sector and not to public bodies.

The GDPR similarly requires DPOs to: (i) inform and advise controllers and processors of their data protection obligations; (ii) monitor compliance; (iii) train staff; (iv) provide advice with respect to and monitor data protection impact assessments; and (v) cooperate with and act as the contact point for supervisory authorities.³⁶⁰

In the HIPCAR Privacy Framework, the data protection officer (called the personal data representative) has to independently ensure that the controller is processing personal data in a lawful and correct manner and in accordance with good practice. The personal data representative would be an independent person within the controller who would have to report non-compliance with data protection obligations to the supervisory authority.³⁶¹ This could be why the CARICOM framework imposes this requirement only on public authorities. According to the OAS Principles, the designation of a Chief Information and Privacy Official within controllers is meant to serve the purpose of controllers adopting effective privacy management programmes, conducting internal reviews and trainings designed to promote the privacy of individuals, and other functions.³⁶²

The GDPR³⁶³ and HIPCAR Privacy Framework³⁶⁴ provide for the independent functioning of the DPOs. Given the range of responsibilities described above, it is essential for DPOs to be able to perform their functions independently. To avoid conflicts of interest and exercise autonomy, DPOs must be provided with the necessary resources and shielded from interference.³⁶⁵

“Although phraseology of DPOs differs, the common responsibility of the DPO across frameworks is to demonstrate or ensure their controllers' compliance with applicable data protection law.”

358 Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines, p 24.

359 Commonwealth PPI Bill, s 21.

360 GDPR, art 39.

361 HIPCAR Model Legislative Text, s 31.

362 OAS Principles with Annotations, principle 10, p 22.

363 GDPR, art 38(3) and recital 97.

364 HIPCAR Model Legislative Text, s 31(2).

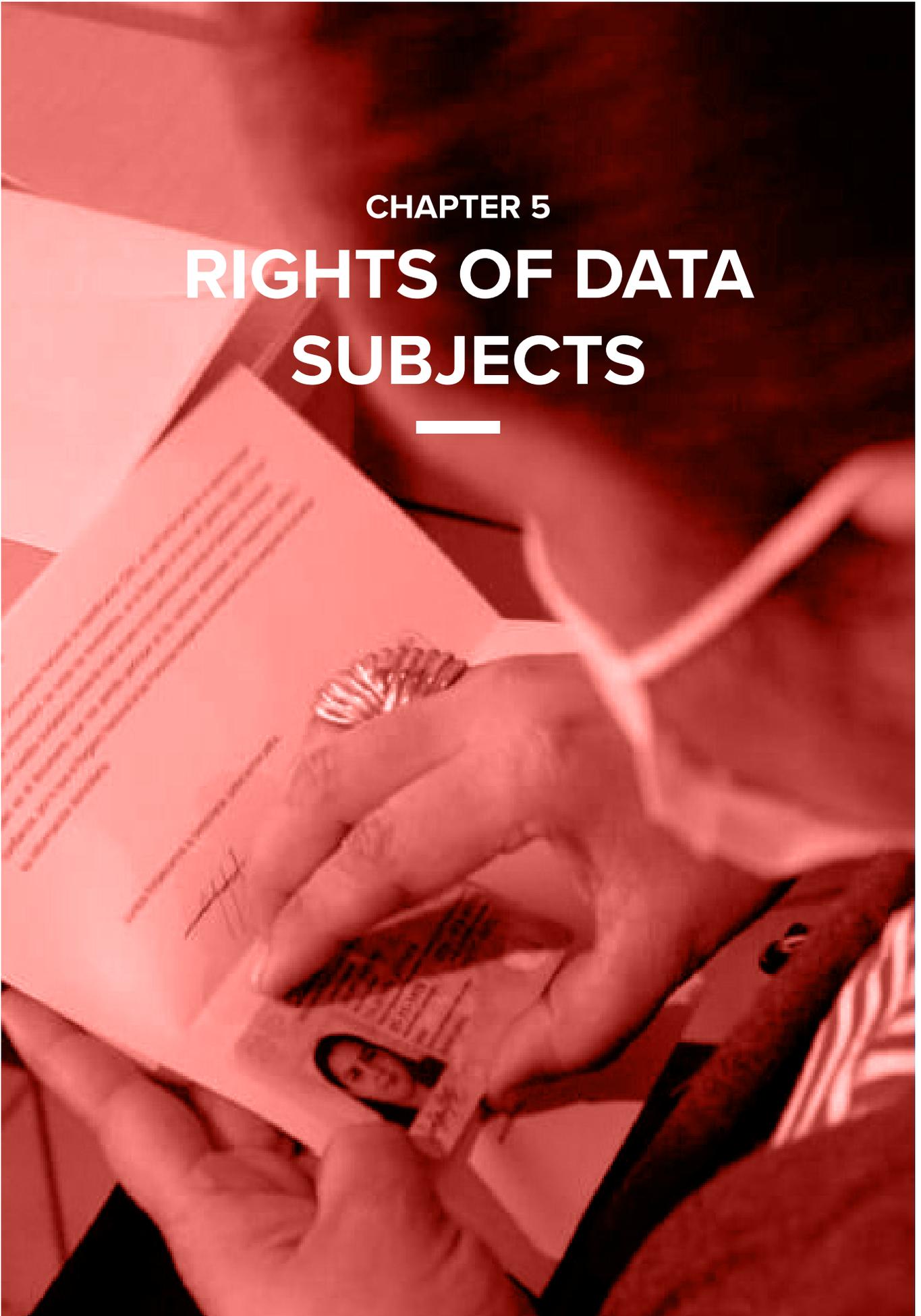
365 Miguel Recio, 'Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability' (2017) 3 Eur Data Prot L Rev 114, p 117.

Key considerations

- ◇ Transparency and accountability measures are essential to effectively implement data protection and operationalise privacy. They complement and support all other components of data protection frameworks and are usually operationalised through the measures discussed in the chapter.
- ◇ Other transparency and accountability measures typically provided for in data protection frameworks include:
 - ◇ **Privacy by design:** It creates accountability and safeguards against risks arising from large-scale processing of personal data, by requiring organisations to proactively embed good privacy practices into the design and operation of systems, infrastructure, and business practices and ensuring privacy and data protection throughout the entire lifecycle of the data.
 - ◇ **Data protection impact assessments (DPIAs):** DPIAs aid in the design and implementation of effective privacy by design systems. They help identify and manage risks arising from data processing activities and take the necessary steps to mitigate those risks.
 - ◇ **Information and access to data:** Information and access requirements for data controllers equips data subjects to effectively exercise their rights and increases accountability. Frameworks typically require controllers and processors to implement a series of practical measures to provide information to data subjects on data processing and management practices, in easily accessible and comprehensible formats.
 - ◇ **Security safeguards:** Data security is a core component of data protection frameworks. All data protection frameworks require controllers to implement data security through technical and organisational measures aimed at protecting the “confidentiality, integrity and availability” of personal data.
- ◇ **Reporting breaches of personal data:** Data breach notification obligations require data controllers and processors to notify supervisory authorities and/or affected data subjects of unauthorised access to data. enables data subjects to mitigate risks, ensures accountability for breaches after they occur, and incentivises controllers to strengthen and maintain strong data security mechanisms.
- ◇ **Maintenance of records:** Maintaining records relating to processing activities forms part of ensuring accountability for controllers and processors, and is a measure of good data governance. It helps organisations demonstrate compliance with data protection laws, and they are ordinarily required to keep a record of their processing activities, including purposes of processing, data retention and sharing activities.
- ◇ **Data protection officers (DPOs):** The appointment of DPOs helps controllers comply with data protection obligations and helps ensure transparency and accountability. DPOs are generally independent and report to the highest management, and usually are required to notify relevant authorities of controllers’ non-compliance with data protection obligations.

CHAPTER 5

RIGHTS OF DATA SUBJECTS



5.1 Introduction

As discussed in Chapter 1 (Introduction), the right to privacy and its various components flow from international instruments like the UDHR and ICCPR, and principles such as the FIPPs. Providing legal rights to data subjects so that they can protect their privacy is one of the ways in which these principles are operationalised. These rights are at the core of data protection frameworks.

This chapter explores the following key rights that are conferred on data subjects in the Identified Regional Frameworks:

- the rights to access, confirmation, and information;
- the rights to rectification and erasure or deletion;
- the rights to be forgotten and to data portability;
- the rights to object and to restrict processing;
- the right against automated decision-making and profiling;
- the right to delegate (or for third-party to exercise) rights; and
- whistle-blower protection.

These rights are meant to provide data subjects with control over their personal information, increase transparency and accountability of data controllers and processors, as well as support data subjects obtain redress for the misuse of their personal data. This chapter also explores the restrictions on these rights along with relevant obligations on data processors.

Most of the Identified Regional Frameworks do not distinguish between data controllers that are private parties, and those that are state entities, for the exercise of data subject rights. The exception is the Commonwealth Privacy Bill, which only focuses on the processing of personal information by state entities. It does not contain specific data subject rights but does include some obligations for data controllers, as covered in Chapters 3 and 4 (on Data Protection Principles, and Transparency and Accountability), and as discussed in relevant sections below. The Commonwealth PPI Bill covers data processing by private sector organisations and provides for data subject rights and controller obligations.

5.2 The rights to access, confirmation, and information

The rights of a data subject to access and confirm the personal information that a data controller possesses about them are among the most basic rights provided by the Identified Regional Frameworks. In fact, the ability to exercise these rights is a necessary first step in meaningfully exercising the other rights available to data subjects: without understanding what information a data controller has about a data subject, the data subject would not be able to assess the ways in which the information is used.³⁶⁶

The Identified Regional Frameworks generally provide for two related rights, namely the right of a data subject to get the data controller to confirm whether it is processing personal information relating to them, and the right to access that personal data. Usually, the right of access and confirmation requires data controllers to provide the relevant information within a reasonable time, either free of charge, or through the payment of a nominal fee. The information must be in a form that is easily understood, and which enables data subjects to either challenge or deny the accuracy of the relevant information.³⁶⁷

Some frameworks contain additional details on how these rights apply for certain kinds of information such as health data, or where automated decision-making technologies are used, as explored below. The right to access and confirmation is not absolute and can be restricted in limited circumstances, such as for legal or statutory duties of confidentiality.

5.2.1 Framework overview of the rights to access, confirmation, and information

There are differences in the way each Identified Regional Framework provides these rights, which are explored below.

5.2.1.1 Confirmation and access

The GDPR, Convention 108+, AU Convention, OECD Guidelines, OAS Principles, and APEC Privacy Framework all contain the rights to confirmation and access, which confirms whether a data controller is processing a data subject's personal information. If a data controller is in possession of an individual's data, it provides the individual the right to access that information and related details.³⁶⁸ The GDPR specifies that this right is provided to data subjects to "be aware of, and verify, the lawfulness of the processing."³⁶⁹ The OECD Guidelines note that the right to access should be simple to exercise, and that there are different ways in which the requirement to communicate requested data within a reasonable timeframe can be satisfied by controllers. Data controllers who provide information to data subjects at regular intervals could, for instance, be exempted from the requirement to respond immediately to individual requests.³⁷⁰ The information to be provided to data subjects pursuant to this right is covered in section 5.2.2 below.

366 Case 553/07 College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer [2009] E.C.R. I-03889 <https://privacylegistry.org/cgcnlud.org/case/college-van-burgemeester-en-wethouders-van-rotterdam-vs-mee-rijkeboer?searchuniqueid=234711>.

367 OAS Principles with Annotations, Principle 8, page 31; APEC Privacy Framework, Part iii, Principle VIII, para 29; Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle, p 58; ASEAN DP Framework, principle 6(e).

368 GDPR, art 15; Convention 108+, arts 9(1)(b), 9(1)(c); AU Convention, arts 16 and 17; Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle, p 58; APEC Privacy Framework, Part iii, Principle VIII, para 29; OAS Principles with Annotations, Principle 8, page 17.

369 GDPR, Recital 63.

370 Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle, p 58.

5.2.1.2 Access

The HIPCAR Privacy Framework and the Commonwealth PPI Bill do not provide data subjects the specific right to confirm whether a data controller has information on them, but they do contain the right to access any information in their custody or control.³⁷¹ However, data controllers under both frameworks are nevertheless required to inform data subjects of the types of data being collected from them and the processing purposes at the time of collection.³⁷² While this would mean that data subjects are ostensibly informed about the fact that a controller has collected their personal information, the Commonwealth PPI Bill also contains provisions allowing data collection without the knowledge and consent of the data subjects in some cases, such as when it is “clearly in the interests of the individual and consent cannot be obtained in a timely manner”.³⁷³ Such exceptions can impair the ability of data subjects to exercise their rights.

5.2.1.3 Access and rectification

The ASEAN DP Framework does not provide for specific rights, but enumerates the principles of data protection, and merges the rights of access and rectification as part of these principles. It couches the rights to access and correction as obligations of data controllers, requiring them to provide data subjects access to their personal data and to correct errors or omissions unless prohibited by law.³⁷⁴ The right to rectification is explored in detail in section 5.3 below.

5.2.2 Information to be provided to data subjects

As noted in Chapter 4 (Transparency and Accountability), the transparency principle requires data controllers to provide data subjects with information such as the fact of collection of personal

data and the purposes of processing. This generally needs to be provided at the time of collection of data or soon thereafter. The right to access information is related but separate, and allows data subjects to access information from controllers on request.

The OCED Guidelines, APEC Privacy Framework, the ASEAN DP Framework, OAS Principles, HIPCAR Privacy Framework, and Commonwealth PPI Bill do not specify the categories of information that are to be made available to data subjects. They simply provide that data subjects should have the right to access, and to have communicated to them the information that a controller has in its possession that relates to the data subjects.³⁷⁵ This information would have to be communicated to the data subject by the relevant controller at the data subject’s request. In contrast, the GDPR, Convention 108+, and the AU Convention require data controllers to provide specific categories of information following a request from the data subject. This includes:

- the categories of personal data processed;
- the purpose for data processing;
- the recipients or categories of recipients to whom the data has been or will be disclosed;
- the period of personal data storage or the criteria used to determine this period;³⁷⁶
- information on the data source when it is not collected from the data subject directly.³⁷⁷

The GDPR and AU Convention also require data controllers to provide information on the existence of other rights available to the data subject, such as the right to rectify or correct information and the right to redress with the relevant national authorities.³⁷⁸

The GDPR and Convention 108+ specify that data subjects have the right to be informed of appropriate safeguards that exist when their personal information is transferred to a third country or international organisation.³⁷⁹ Such measures can help provide

371 HIPCAR Model Legislative Text, s 22; Commonwealth PPI Bill, s 22.

372 HIPCAR Model Legislative Text, s 9, 10; Commonwealth PPI Bill, s 8 and s 9.

373 Commonwealth PPI Bill, s 11.

374 ASEAN DP Framework, principle 6(e).

375 Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle; ASEAN DP Framework, principle 6(e); OAS Principles with Annotations, Principle 8, page 17; APEC Privacy Framework, Principle VIII, para 29; HIPCAR Model Legislative Text, s 22(1); Commonwealth PPI Bill, part IV and s 22.

376 GDPR, art 15; Convention 108+, art 9(1)(b); AU Convention, art 16.

377 GDPR, art 15; Convention 108+, arts 9(1)(b) and 8(1); AU Convention, art 17(c).

378 GDPR, arts 15(1)(e)-(f); AU Convention, arts 16 (e)-(f).

379 GDPR, art 15(2); Council of Europe, ‘Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data’ (1981), [68] (Explanatory Report –Convention 108+).

data subjects with more control to decide how their personal information is used and the kinds of data processing acceptable to them.

While most frameworks require information to be provided in an easily understood format, a few specifically require controllers to provide information in alternative formats for data subjects with disabilities.³⁸⁰ The OAS Principles specify that domestic law should provide mechanisms by which access to information should be provided to groups at greater disadvantage or who face greater risks of exclusion. It also notes that exercising these rights should not result in discrimination, denial of service, or differential service to data subjects.³⁸¹

5.2.3 Controller obligations to provide information to data subjects

Some of the requirements outlined above are framed as controller obligations in some frameworks, as outlined in Chapter 4 (Transparency and Accountability). More generally, transparency and accountability obligations imposed on data controllers are complementary to the rights to confirmation and access. The Commonwealth Privacy Bill requires that public authorities collect data only for lawful purposes and when data collection is necessary for those purposes. They must take “reasonable” steps to ensure that the relevant data subjects are made aware that some of their personal information is being collected at the time it is obtained, or soon thereafter. The purposes of collection and the intended recipients should also be communicated to data subjects at the time of collection and thereafter. It also requires that the authorities take reasonable steps to ensure the accuracy of the information, limit its use and disclosure with certain exceptions, and ensure the storage and security of personal information.³⁸²

5.2.4 Information to be provided on automated decision-making

As noted in Chapter 4 (Transparency and Accountability), the GDPR and Convention 108+ require data controllers to share information about: (i) the existence of automated decision-making technologies, including information about profiling; (ii) the logic underlying such processing; and (iii) the significance and anticipated consequences of such processing for the data subject.³⁸³ This is based on the understanding that having access to such information contributes to the data subject’s ability to exercise other rights and to avail themselves of safeguards, such as the right to object to personal data collection and to complain to the relevant supervisory authority. Data subjects would therefore be able to contest the logic underlying automated processing that is applied to them, such as for credit scoring, providing benefits, etc.

The OECD Guidelines highlight the practical challenges that may arise when implementing the right to access and correction in the digital age. For instance, it is not clear how data subjects would exercise the right to access their information from a platform undertaking a street mapping exercise. In the context of automated risk management and profiling, the Guidelines point out that it is essential for information to be accurate and up to date due to the increasing reliance on transactional data for automated risk management and profiling. In this context, authenticating the identity of individuals who are exercising this right with no prior relationship with the relevant organisation could be especially challenging.³⁸⁴

380 Convention 108+, Art 9(1)(b); Explanatory Report – Convention 108+, [68] and [76]; APEC Privacy Framework, Part iii, Principle VIII, para 29(b)(iv); OAS Principles with Annotations, Principle 8, page 18; Original Explanatory Memorandum OECD Guidelines, Individual Participation Principle, para 13(b)(iv), GDPR, recitals 39, 58; Commonwealth PPI Bill, s 26; HIPCAR Model Legislative Text, s26(2).

381 OAS Principles with Annotations, Principle 8, pages 18-19.

382 Commonwealth Privacy Bill, ss 9-14.

383 GDPR, art 15; Convention 108+, art 9(1)(c)

384 OECD, ‘The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines’ in OECD (ed), *The OECD Privacy Framework* (2013), 100-101.

5.2.5 Information to be provided on health data

Typically, frameworks provide that data subjects can approach data controllers to exercise the rights to access and confirm personal information. However, Convention 108+ and OECD Guidelines recognise that in some cases, it may be more appropriate to provide for access to personal data through an intermediary. For example, where health data is concerned, it may be appropriate for a data subject to use the assistance of a health professional to exercise their right to access their health information.³⁸⁵ Convention 108+ notes that the health professional could assist in helping the data subject understand the information, or in ensuring that their psychological state is accounted for when receiving sensitive information. Such measures can be very helpful in meaningfully exercising the right to access and information, since the data subject would be able to rely on expert assistance to understand the information that is made available to them. Convention 108+ also specifies that an intermediary to the supervisory authority may be involved in exercising this right “in exceptional circumstances”, though it does not provide information on the circumstances in which this may be beneficial.³⁸⁶

The GDPR also addresses health data and specifies that data subjects must have the right to access information concerning their health, such as information included in their medical records.³⁸⁷



385 Explanatory Report – Convention 108+, [74]; Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle, p 58.

386 Explanatory Report – Convention 108+, [74].

387 GDPR, recital 63.

5.2.6 Denial of information requests from data subjects

Data controllers can in some circumstances deny requests made under this right. However, per Convention 108+, the OAS Principles, the GDPR, and the OECD Guidelines, they would be required to provide the data subjects with justifications for denial of requests, and the OAS Principles and OECD Guidelines require data subjects to be allowed to challenge denials for information.³⁸⁸ This provision exists in addition to the general ability of data subjects under most Identified Regional Frameworks to lodge complaints with the relevant data protection authority with regards to possible violations of the relevant frameworks.³⁸⁹

Within this context, the OAS Principles require data controllers to have an effective method by which data subjects can be made aware of the reasons for a denial of information and challenge the decision. This is to prevent arbitrary rejections and to allow data subjects to correct errors and mistakes, which is seen as a fundamental right under some frameworks.³⁹⁰ The OECD Guidelines specify that the right to challenge denial of information is broad enough to include not only initial challenges to the data controller, but also subsequent challenges according to domestic procedures in front of the courts, administrative bodies, and other bodies. The data subject would be entitled to the reliefs determined by law and domestic procedure in such cases.³⁹¹

Importantly, the OECD's Expert Group that drafted the Guidelines contemplated broadening the right to obtain reasons for any adverse decisions relating to the use of personal data, beyond denials of requests under the right to access and confirmation. However, it ultimately decided that it was too broad to be

included in the framework. Nevertheless, the OECD Guidelines recognise that a right to obtain reasons for adverse decisions to data subjects based on the use of personal data, broader than in the context of access to information, may be appropriate and enable data subjects to effectively exercise their rights.³⁹²

5.2.7 Exemptions to the rights to access, confirmation, and information

The AU Convention, Convention 108+, and the OECD Guidelines do not contain specific exemptions to the rights to access, confirmation and information. The OAS Principles note that exceptional situations exist that would require personal data to be kept confidential. It provides that the restrictions should be set out in appropriate legislation or other instruments and should be as narrow and restrictive as possible. It provides an illustrative list of circumstances in which the restrictions should apply, such as where it would compromise trade secrets, or when a data subject is suspected of wrongdoing and is the subject of law enforcement investigations.³⁹³

388 OAS Principles with Annotations, Principle 8, page 17; GDPR, recital 59, art 12 (3,4); Explanatory Report – Convention 108+, [76]; OECD Guidelines, Paragraph 13(c) – Individual Participation Principle, Original Explanatory Memorandum OECD Guidelines, Paragraph 13 – Individual Participation Principle, p 59.

389 GDPR, art 77; Convention 108+, arts 12 and 15(4); Explanatory Report – Convention 108+, [99]-[100], [122]; AU Convention, art 12(2)(e) (framed as a duty of the supervisory authority); OAS Principles with Annotations, Principle 13, page 27; HIPCAR Model Legislative Text, part VI; Commonwealth PPI Bill, s 29 (framed as a duty of the supervisory authority); Original Explanatory Memorandum OECD Guidelines, Paragraph 19 – National Implementation; APEC Privacy Framework, para 53. The ASEAN DP Framework does not specifically describe remedies but requires that organisations should be accountable for complying with measures which give effect to the principles (ASEAN DP Framework, principle 6(h)).

390 OAS Principles with Annotations, Principle 8, page 19.

391 Original Explanatory Memorandum OECD Guidelines, p 58.

392 Original Explanatory Memorandum OECD Guidelines, p 59.

393 OAS Principles with Annotations, Principle 8, pages 18-19.

The other frameworks provide specific exceptions to these rights, which include:

- Contravention of the rights and freedoms of others in some contexts, such as the invasion of another individual's privacy, the life or security of another individual, or health data that could harm the health and safety of any individual;³⁹⁴
- Information relating to investigations, breach of law, or subject to confidentiality obligations, or if provided by law;³⁹⁵
- Information that would reveal confidential information that could reasonably be expected to harm the data controller or reveal trade secrets and other similar information;³⁹⁶
- Unreasonable or repetitive requests from a data subject that would impose disproportionate costs, the identity of the requester is not established, or the requests are made in bad faith.³⁹⁷

Where some information requested by the data subject is exempt from disclosure, the HIPCAR Privacy Framework and APEC Privacy Framework require controllers to sever information which is exempt, and make the non-exempt information available to data subjects.³⁹⁸

The GDPR only specifically restricts the right of data subjects to access their personal information when the rights and freedoms of others are affected. However, as discussed in Chapters 3 and 4 (on Data Protection Principles, and Transparency and Accountability), controllers must provide certain information to data subjects when collecting personal data. The GDPR provides additional exemptions to this obligation when the controllers obtain personal data from sources other than the data subjects themselves. Exemptions would apply when the data subject already has the relevant information, when it involves a disproportionate effort to provide such information, especially when processing occurs for

specific purposes as provided by law, and other specified circumstances.³⁹⁹

The Commonwealth PPI Bill also contains a provision that is not contained in other frameworks. If an organisation receives a request to access personal information that was previously disclosed to a governmental agency, the organisation is required to provide the agency written notice of the request. If the governmental agency objects to the request, the organisation is not allowed to provide the relevant information to the data subject.⁴⁰⁰ The Bill does not specify whether the data subject should be informed of the reason for the denial of their information request. Such provisions could significantly restrict the data subjects' right of access, especially when they are unaware of the reasons for information denial.

“the ability to exercise these rights (i.e. the rights of data subject to access and confirm the personal information) is a necessary first step in meaningfully exercising the other rights available to data subjects.”

394 GDPR, art 15(4); HIPCAR Model Legislative Text, s 23(1)(a) and 23 (1)(d). See also APEC Privacy Framework, Principle VIII, para 30(iii); Commonwealth PPI Bill, s 22(1).

395 HIPCAR Model Legislative Text, s 23(1)(c); Commonwealth PPI Bill, s 22(1); APEC Privacy Framework, principle VIII and para 30(ii); ASEAN DP Framework, principle 6(e)(ii).

396 Commonwealth PPI Bill, s 22(1). The APEC Privacy Framework also exempts disclosure that would benefit a competitor – see APEC Privacy Framework, commentary to Principle VIII and paras 29-31.

397 HIPCAR Model Legislative Text, s 23(2); Commonwealth PPI Bill, s 23(6). See also APEC privacy framework, principle VIII and para 30(i) and related commentary.

398 HIPCAR Model Legislative Text, s 24; APEC Privacy Framework, commentary to Principle VIII and paras 29-31.

399 GDPR, art 14(5) and 15(4).

400 Commonwealth PPI Bill, s 22(6).

5.3 The rights to rectification and erasure or deletion

All Identified Regional Frameworks contain a right to rectification. This is among the most important rights for data subjects since inaccurate data can lead to exclusions, inaccurate decisions, and other harms based on the nature of data and processing. Most of them also provide the right to erase information in some contexts, as discussed below. These rights permit data subjects to require the data controller to rectify or erase personal information, which has been processed in contravention of applicable law, or when the information is inaccurate or incomplete.⁴⁰¹ They also usually require the data controllers to notify other recipients with whom the controllers have shared the data of such rectification or deletion when possible. Data controllers have the discretion to refuse to comply with rectification or erasure requests when they are not satisfied with the data subject's claim or in other limited circumstances. The right allowing for information to be erased in the context of rectification as presently described is distinct from the GDPR's conception of the right to be forgotten.

5.3.1 Framework overview of the rights to rectification and erasure or deletion

All Identified Regional Frameworks provide data subjects the right to rectify information that a data controller possesses about them.⁴⁰² Convention 108+, the AU Convention, and the APEC Privacy Framework also provide the right to erase data. However, the OAS Principles also specify that there may be some situations in which it may be more appropriate for data controllers to add more information to their existing records to accurately reflect the history of the information rather than to delete it.⁴⁰³

Interestingly, the OECD Guidelines specify that the data subject's right to challenge the personal data held by data controllers does not imply that they are able to choose the remedy, such as to rectify the information, erase data, or annotate that the data is in dispute, but that it must be determined by domestic law and regulation. The HIPCAR Privacy Framework references the OECD's Individual Participation Principle, which allows for data to be erased, rectified, completed, or amended when it is successfully challenged, but does not contain a specific right to erasure.⁴⁰⁴

401 AU Convention, art 19; HIPCAR Model Legislative Text, s 27; ASEAN DP Framework, principle 6(e)(ii); OAS Principles with Annotations, Principle 8, page 19; Commonwealth PPI Bill, s 28; APEC Privacy framework, para 29(c).

402 GDPR, art 16; HIPCAR Model Legislative Text, s 27(1); Commonwealth PPI Bill, s 28(1); Convention 108+, art 9(1)(e), Explanatory Report - Convention 108+, [72]; AU Convention, art 19; ASEAN DP Framework, principle 6(e); OAS Principles with Annotations, Principle 8, page 19; APEC Privacy Framework, principle VIII and para 29(c); Original Explanatory Memorandum OECD Guidelines, Paragraph 13(d) – Individual Participation Principle.

403 Convention 108+, art 9(e). The explanation specifies that this includes the right to the right to rectify or erase inaccurate, false, or unlawfully processed data (Explanatory Report - Convention 108+, [72]); AU Convention, art 19; APEC Privacy Framework, principle VIII and para 29; OAS Principles with Annotations, Principle 8, page 19.

404 OECD, 'Original Explanatory Memorandum to the OECD Privacy Guidelines (OECD, 1980)' in OECD (ed), The OECD Privacy Framework (2013), p 59 (Original Explanatory Memorandum OECD); HIPCAR, 'Explanatory Notes to Model Legislative Text on Privacy and Data Protection' in HIPCAR (ed), Privacy and Data Protection - Model Policy Guidelines and Legislative Text (HIPCAR, 2012), [15] and [34]. It also allows for the Authorities to order data controllers to rectify or erase information ([68]).

5.3.2 Notice of rectification

Convention 108+ and the GDPR specifically require that data controllers notify other recipients with whom the controllers have shared the data of any rectification that takes place. The HIPCAR Privacy Framework goes further and requires controllers to annotate the data with the relevant requests when they are made, and to notify other data controllers and third parties to whom the data was disclosed to one year prior to the request. Other controllers or third parties must also similarly correct or annotate the personal data if it is still in their custody or control. The Commonwealth PPI Bill similarly requires controllers to “ensure that it does not obliterate the text of the record” as it existed before correction, where practicable. The OAS Principles explicitly caution that data subjects must not be allowed to introduce incorrect information into the controller’s records.⁴⁰⁵

5.3.3 Refusal of requests for rectification and erasure or deletion

All Identified Regional Frameworks provide data subjects the rights to access and correction, and a few also explicitly recognise these rights as among the most important safeguards to protect an individual’s privacy.⁴⁰⁶ However, data controllers can also refuse to comply with rectification or erasure requests when:⁴⁰⁷

- they are not satisfied of the data subject’s claim;
- it is required or authorised by law;
- necessary to protect commercial interests;
- the general exceptions to the rights of data subjects apply.

The rights of a data subject to access information and rectify any errors are likely the most important rights from the perspective of public bodies, as well as to establish digital identities. This is both because these rights are the basis to meaningfully exercise other rights available to data subjects, and because they can lead to significant consequences for data subjects depending on the nature of the data and its use.

Digital ID systems use individuals’ information to identify them and authorise systems to interact with them, and any errors in such information can lead to exclusions. The consequences of inaccurate information can be particularly severe if it is the basis to access services or decisions that can significantly affect the data subject. To be effective, it is essential that the rights to rectification and erasure can also be enforced against the state and public bodies. It is therefore essential for digital ID systems to be situated within a robust data protection framework and to be established pursuant to legislation that takes into account these concerns. It is also important for data protection authorities to operate independently, and to enforce data subject rights against state actors.

5.3.4 Exemptions to the rights to rectification and erasure or deletion

The OAS Principles note that the right to rectification or correction is not absolute and can be restricted when personal data is legally required to be retained by national legislation for the carrying out of an obligation, among other circumstances. It notes that national legislation must specify the conditions of access and rectification, applicable restrictions, and the specific grounds for such restrictions.⁴⁰⁸

405 Explanatory Report - Convention 108+, para 81; GDPR, art 19; HIPCAR Model Legislative Text, ss 27(3) - (4); Commonwealth PPI Bill, s 28(3); OAS Principles with Annotations, Principle 8, page 19.

406 Original Explanatory Memorandum OECD Guidelines, [13], p 58; OAS Principles with Annotations, Principle 8, page 19; APEC Privacy Framework, commentary to Principle VIII and paras 29-31.

407 Commonwealth PPI Bill, s 28(1); ASEAN DP Framework, principle 6(e)(ii); OAS Principles with Annotations, Principle 8, page 19; The APEC Privacy Framework provides additional grounds, APEC Privacy Framework, commentary to Principle VIII and paras 29-31.

408 OAS Principles with Annotations, Principle 8, page 19.

5.4 The rights to be forgotten and to data portability

“some frameworks provide data subjects the right to erase personal information held by data controllers”

The GDPR and the OAS Principles engage with these rights. The GDPR provides an explicit right to be forgotten. Nevertheless, several national authorities in other jurisdictions have also engaged with it in certain contexts, and the OAS Principles have acknowledged the right without explicitly providing for it. The GDPR and OAS Principles also provide the right to data portability.

5.4.1 The right to be forgotten

As discussed in the section above, some frameworks provide data subjects the right to erase personal information held by data controllers. This right can typically be exercised when the data subject’s personal information is inaccurate or incomplete, or where the data has been unlawfully processed. The GDPR provides a separate “right to be forgotten”, which allows data subjects to request that their information be erased in specified circumstances. It is not an absolute right, and can be exercised in broader range of situations, such as when the personal data is no longer necessary for the purpose for which it was collected or when the data subject withdraws consent to processing or objects to the processing pursuant to the right to object, or if the personal data has been unlawfully processed, among other circumstances.⁴⁰⁹ In the context of the internet, the right to be forgotten is typically exercised to remove information relating to a data subject from results of search engines and websites.⁴¹⁰

⁴⁰⁹ GDPR, art 17.

⁴¹⁰ See for example Case C-131/12 Google Spain v AEPD [2014] OJ C 212 (Google v Spain) <https://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>; Case C-507/17 Google v CNIL [2019] ECLI:EU:C:2019:15 <https://privacylibrary.ccgnlud.org/case/google-llc-vs-commission-nationale-de-linformatique-et-des-liberts-cnil>; and Case C-136/17 GC and Others v CNIL [2019] ECLI:EU:C:2019:773 (GC v CNIL) <https://privacylibrary.ccgnlud.org/case/gc-af-bh-ed-vs-commission-nationale-de-linformatique-et-des-liberts-cnil>.

In terms of search engines, this has manifested itself as a right to de-list information, meaning that data subjects can require search engine operators to not display links to certain information in search result. Given the potential implications on other rights such as freedom of speech and access to information, the GDPR provides for situations in which this right would not apply, such as when the processing is necessary to exercise the right of free speech, complying with legal obligations, and other such circumstances.⁴¹¹ Data controllers would have to take these and various other factors into account when assessing whether to erase information pursuant to a data subject's request.⁴¹²

5.4.1.1 Framework overview of the right to be forgotten

Although versions of this right have existed before, the right to be forgotten was brought into prominence in 2014. In *Google v Spain*, the ECJ found that data subjects could require search engines to remove personal data from search results, when the linked information was “inadequate, irrelevant or no longer relevant, or excessive”.⁴¹³ It noted that search engines had the ability to significantly affect a person's right to privacy since any internet user had the ability to obtain a wide range of information on a person's life which would otherwise have been inaccessible.⁴¹⁴ The GDPR highlights the importance of this right when data subjects consent to processing of information as children, which is at a time they are not fully aware of the risks and implications of online processing. It allows them to subsequently withdraw their consent from processing and to remove the relevant personal information from the internet. It also specifies that whenever exercised, the data

controllers who made the personal data public must take reasonable steps to inform other data controllers processing the information to erase links and copies to the information.⁴¹⁵

The OAS Principles also engage with the right to be forgotten and note that some national schemes provide data subjects with the right to erase publicly available data when it is “no longer necessary or relevant”, or in the case that they object to or withdraw consent to processing. They recognise that this right involves balancing different interests and principles, not only of privacy, but of “access to truth, freedom of information and speech, (and) proportionality”. They note that states should use national legislation to establish this right “where appropriate”, along with the terms of its use and exemptions. They note, however, that it remains contentious and is subject to differing definitions and conceptions of personal data, especially when it concerns factual data that is nevertheless considered excessive, personally embarrassing, or irrelevant by the data subject.⁴¹⁶

5.4.1.2 Scope of the right to be forgotten

The right to de-list information as formulated by ECJ jurisprudence does not require search engines to delete the relevant information, but instead to significantly restrict access to it online.⁴¹⁷ The Court more recently provided guidance to data controllers with regards to factors that they would have to consider when assessing requests to delist information, which would require them to strike a “fair balance” between the data subject's right to respect for private life and the public's freedom of information.⁴¹⁸ It also requires search engine operators to assess the relevance of information relating to previous

411 GDPR, art 17(3).

412 ECJ case law provides some guidance: see for example Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:15 <https://privacylibrary.ccg.nlud.org/case/google-llc-vs-commission-nationale-de-linformatique-et-des-liberts-cnild>; and Case C-136/17 *GC and Others v CNIL* [2019] ECLI:EU:C:2019:773 (*GC v CNIL*) <https://privacylibrary.ccg.nlud.org/case/gc-af-bh-ed-vs-commission-nationale-de-linformatique-et-des-liberts-cnild>. See also Article 29 Data Protection Working Party, ‘Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Española De Protección De Datos (Aepd) and Mario Costeja González” C-131/12’ (2014) <https://privacylibrary.ccg.nlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>.

413 Case C-131/12 *Google Spain v AEPD* [2014] OJ C 212 (*Google v Spain*) <https://privacylibrary.ccg.nlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>.

414 *Google v Spain*, [35] – [38] <https://privacylibrary.ccg.nlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>.

415 GDPR, recitals 65-66.

416 OAS Principles with Annotations, Principle 8, page 20.

417 *Google v Spain*, [88] <https://privacylibrary.ccg.nlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>.

418 *GC v CNIL*, [53, 66, 76, 77] <https://privacylibrary.ccg.nlud.org/case/gc-af-bh-ed-vs-commission-nationale-de-linformatique-et-des-liberts-cnild>. See also *Google v Spain*, [81, 99] <https://privacylibrary.ccg.nlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd>.

criminal proceedings brought against data subjects in responding to requests for de-referencing such information against factors such as the seriousness of the offence, the public's interest in the information, and the amount of time that has elapsed since the offence. Search engines would have to nevertheless reorder search results, such that "the overall picture it gives the internet user reflects the current legal position", meaning, in particular, that web pages with information on the updated legal status (such as acquittal, conviction, appeal, etc) must appear in first on in search results.⁴¹⁹

National authorities in other jurisdictions such as India, South Africa, and Canada have contemplated including versions of this right in their domestic legislation.⁴²⁰ It has sometimes been explored as a right to be provided by state actors, or the judiciary, instead of by data controllers. For instance, India's draft Data Protection Bill, 2021 requires regulatory officers appointed under the legislation to assess data subject requests to exercise this right.⁴²¹ In many jurisdictions, petitioners have also approached courts seeking personal information to be removed. Courts have also referenced the right to be forgotten in providing remedies, even when a specific right has not been provided by legislation.⁴²²

5.4.1.3 Threats to access to information under the right to be forgotten

While the right to be forgotten can provide for the effective enforcement of a data subject's privacy rights, especially online, it can also have certain implications for the rights to free speech and access to information. Most of the concerns about this right stem from its ability to impede access to information and that this, in turn, has the potential to lead to the withholding of critical information. There are also concerns that this right could lead to the removal of sources of factual information and thereby threaten deliberation in the public sphere, which is essential to democratic governance.⁴²³

In addition, there are concerns that the GDPR's conception of the right to be forgotten places undue responsibility on search engines to make assessments on permitted speech and raises other practical difficulties.⁴²⁴ An alternative aimed at addressing this concern is reflected in India's Data Protection Bill, 2021. It requires data subjects to approach adjudicating officers appointed under the data protection legislation to exercise this right. These officers are required to account for considerations laid down in the Bill, and are also required to have special knowledge of or professional experience in

- 419 GC v CNIL, [77-78] <https://privacylibrary.ccg.nlud.org/case/gc-af-bh-ed-vs-commission-nationale-de-linformatique-et-des-liberts-cnll>.
- 420 See for instance considerations in Canada: Law Library of Congress (US) Global Legal Research Directorate, *Laws on erasure of online information*: Canada, France, European Union, Germany, Israel, Japan, New Zealand, Norway, Portugal, Russia, Spain, United Kingdom (2017) 33-35. Indian Personal Data Protection Bill 2019, clause 20 (Indian DP Bill). See South African Protection of Personal Information Act 2013, s 5.
- 421 Indian Data Protection Bill 2021, clause 20 (Indian DP Bill). This draft Personal Data Protection Bill, 2019 has been withdrawn, and the government is expected to present a new bill that aligns with a "comprehensive legal framework" on the digital ecosystem. See Soumyarendra Barik, 'Govt withdraws data protection Bill to bring revamped, refreshed regulation', *The Indian Express*, 5 August 2022, <https://indianexpress.com/article/india/government-withdraws-data-protection-bill-8068257/>.
- 422 See for instance in Turkey, where the right was recognised in the context of restricting the publication of the name of a survivor of sexual assault in a criminal law book: Deris, 'Turkey: The Supreme Court Decision on the Right to be Forgotten' (mondaq.com, 12 November 2019) <https://www.mondaq.com/advicecentre/content/3110/The-Supreme-Court-Decision-on-the-Right-to-be-Forgotten>; India: On varying approaches taken by High Courts in the context of restricting information relating to lawsuits online – Amber Sinha, 'Right to be Forgotten: A Tale of Two Judgements' (cis-india.org, 7 April 2017) <https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments>; Subhranshu Rout @ Gugul v. State of Odisha BLAPL No 4592 of 2020; Zulfiqar Ahman Khan v Quintillion Business Media [2019] (175) DRJ 660, [8]-[9]. See also, Lydia Suzanne Thomas, 'Information in public domain is like toothpaste, can't get it back once it is out of the tube: Orissa High Court calls for right to be forgotten' (barandbench.com, 24 November 2020) <https://www.barandbench.com/news/litigation/orissa-high-court-calls-for-debate-on-right-to-be-forgotten>.
- 423 Access Now, 'Access Now Position Paper: Understanding the "Right to Be Forgotten" Globally' (2016); See Case C-507/17 Google v CNIL [2019] ECLI:EU:C:2019:15 <https://privacylibrary.ccg.nlud.org/case/gc-af-bh-ed-vs-commission-nationale-de-linformatique-et-des-liberts-cnll>; Alexander Tsesis, "'Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure' [2019] 90 University of Colorado Law Review 593, 620 and 621.
- 424 James Ball, "'Right to be forgotten' ruling creates a quagmire for Google et al' (theguardian.com, 13 May 2014) <https://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google>. See also Jeffery Rosen, 'The Right to Be Forgotten' [2012] 64 Stan L Rev Online 88 <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>.

areas relating to law and policy as prescribed by the state,⁴²⁵ and they could therefore be better placed to make such assessments. Although such a model may address some concerns, the implementation of the right to be forgotten would depend on whether the adjudicating officers are able to function independently, especially when the exercise of this right relates to governmental actors or actions.

5.4.1.4 Exemptions to the right to be forgotten

The GDPR limits the right to erasure in certain contexts, such as to exercise the right to free speech and information, compliance with a legal obligation, public interest, archiving, research, and related purposes, or for actions relating to legal claims.⁴²⁶

5.4.2 Right to data portability

The GDPR provides data subjects with the right to obtain the personal data they have provided to a data controller and transmit it to another data controller. This right only applies to personal data provided by the relevant data subject, where the controller carries out the data processing by automated means, and where the processing is based on the data subject's consent or is necessary for the performance of a contract.⁴²⁷ This right can support the fostering of interoperability and competition in the context of digital platforms, whereby consolidation of market power among a few platforms is a significant concern.⁴²⁸ However, this right would not be applicable to processing, necessary for tasks carried out in public interest, or in exercise of official authority vested in a controller.⁴²⁹ Therefore, most state action would be exempt from this right.

The OAS Principles note that the right to data portability is subject to ongoing discussion amongst OAS Member States, most of whom agree that data subjects must be able to avail themselves of this right when personal data is processed digitally or through automated means. They note that this right must not have negative impacts on the rights and freedoms of others, and that it would not be justified when it involves information inferred, derived, or created through processing or analysis conducted by the relevant data controller.⁴³⁰

425 Indian DP Bill 2021, clauses 20, 63(3).

426 GDPR, art 17(3).

427 GDPR, art 20.

428 See Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (2016), pp3-4. See generally Paul De Hert et al, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' [2018] 34(2) Computer Law & Security Review 193.

429 GDPR, art 20(3) and 20(4).

430 OAS Principles with Annotations, Principle 8, page 20.

5.5 The rights to object and to restrict processing

A right that is related to the rights to restriction on processing and erasure, but is nevertheless separate and distinct is the right to object to processing.⁴³¹ The right to object prevents further processing for one or more specified purposes. The right to restrict processing is usually a temporary measure taken when the data controller is contemplating requests by the data subject to rectify or objections to use of personal information.

5.5.1 The right to object

The GDPR, OAS Principles, Convention 108+, AU Convention, and the HIPCAR Privacy Framework provide data subjects the right to object.⁴³² Of these, all frameworks other than the HIPCAR Privacy Framework specifically provide that data subjects may object to data processing for marketing purposes. Though the right is framed broadly, allowing data subjects to object to object to data processing by controllers, it generally applies to processing undertaken on the basis of factors other than consent (for example, in public interest or for direct marketing). Where the data processing is based on consent, data subjects are typically able to withdraw their consent.

The GDPR allows the data subject to object to the controller processing personal data concerning them which is based on specific grounds: (i) processing necessary for performing a task in the public interest or exercising official authority vested in the controller;

(ii) processing for legitimate interests pursued by the controllers or third parties, except where these interests are overridden by the rights and freedoms of the data subject;⁴³³ and (c) direct marketing and individual profiling related to such marketing.⁴³⁴

According to the GDPR, Convention 108+, and OAS Principles, personal data must no longer be used when the data subject objects to processing for the purpose of marketing. Other frameworks provide data subjects the right to object as well, and it can usually be exercised on legitimate grounds as it relates to a data subject.⁴³⁵

The UK Information Commissioner's Office clarifies with respect to the GDPR that the data subject can object to all the personal data that a controller is processing about them, or only some information, or only information relating to a certain purpose that a controller is processing information for. If a data subject objects to processing and a data controller does not have valid grounds to refuse it, it will be required to stop processing that data.⁴³⁶ As with the right to restrict processing, the actions to be taken by the data controller would depend on how it is processing the data in question. The AU Convention specifically provides the right to be informed before the personal data relating to a data subject is disclosed to third parties for the first time or used on their behalf for marketing, and to object to such disclosure or use.⁴³⁷

431 Explanatory Report –Convention 108+ [78].

432 GDPR, art 21; OAS Principles with Annotations, Principle 8, page 20; Convention 108+, art 9(1)(d); AU Convention, art 18; HIPCAR Model Legislative Text, s 9(2).

433 This can range from the data controller's own interests to that of third parties, commercial interests, and larger societal benefits, as long as they override the individual's interests. See UK Information Commissioner's Office, 'Right to Object' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/#ib2>.

434 GDPR, art 21.

435 GDPR, art 21; Explanatory Report –Convention 108+ [79]; OAS Principles with Annotations, Principle 8, page 20. See also UK Information Commissioner's Office, 'Right to Object' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/#ib4>; Convention 108+, art 9(1)(d) and [79]; AU Convention, art 18; HIPCAR Model Legislative Text, s 9(2).

436 UK Information Commissioner's Office, 'Right to Object' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>.

437 AU Convention, art 18.

5.5.1.1 Exemptions to the right to object

The GDPR and Convention 108+ detail specific exemptions to the right to object. The right would not be available when the data controller demonstrates legitimate grounds for the processing which override the rights and interests of the data subject. The legitimate grounds could include factors such as the establishment of legal claims and public safety, which would have to be demonstrated on a case-to-case basis.⁴³⁸ Convention 108+ also highlights that the right to object could be limited through a law, such as to investigate or prosecute criminal offences. The data subject could nevertheless obtain similar reliefs by challenging the lawfulness of the processing itself, or withdrawing consent for processing, or revoking the contract on which the processing is based. However, in such cases, the data subject would have to assume the consequences of such actions, including potentially compensating the controller.⁴³⁹

5.5.2 The right to restrict processing

The GDPR is the only framework that provides for this right, and it allows the data subject to require the controller to restrict the processing of their personal data in some circumstances. Usually, this would be temporary, and apply in some situations, such as when the data subject contests the accuracy of personal data or exercises the right to object, and the controller considers the request, and other specified circumstances.⁴⁴⁰



438 Convention 108+, art 9(1)(d); GDPR, art 21; See also the UK ICO's discussion on what would constitute 'legitimate interests' at UK Information Commissioner's Office, 'Legitimate interests' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/#ib2>; Explanatory Report –Convention 108+ [78].

439 Explanatory Report –Convention 108+ [80].

440 GDPR, art 18.

5.6 The right against automated decision-making and profiling

“Automated decisions involve decisions made by automated means without human involvement.... ”

The GDPR, Convention 108+, and AU Convention provide data subjects with the right to not be subject to a decision based solely on automated processing, including profiling, which would produce legal effects or significantly affect them. The GDPR provides examples of what such significant effects could be, such as the automatic refusal of an online credit application, or e-recruiting practices undertaken without human intervention.⁴⁴¹

Automated decisions involve decisions made by automated means without human involvement, such as recruitment tests that use pre-programmed algorithms and criteria to test aptitude.⁴⁴² In the GDPR and Convention 108+, automated decision-making also specifically includes profiling, which is automated processing that evaluates personal aspects relating to a data subject, such as their economic situation, performance at work, health, location, etc.⁴⁴³ This right also allows data subjects to challenge the decision arrived at by such a process and offer their own points of view and arguments.⁴⁴⁴

441 GDPR, art 22 and recital 71; Convention 108+, art 9(1)(a); AU Convention, art 14(5).

442 Information Commissioner’s Office, ‘Rights related to automated decision making including profiling’ (ico.org.uk) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.

443 GDPR, arts 4(4) and 22; Convention 108+, art 9(1)(a). See also Article 29 Data Protection Working Party, ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679’ (2018).

444 The GDPR and Convention 108+ specifically allows data subjects to challenge the decisions arrived at in this manner and offering their own views. Explanatory Report - Convention 108+, paras 75-77; GDPR, recital 71. The AU does not specifically allow for this – see AU Convention, art 14(5).

5.6.1 Framework overview of the right against automated decision-making and profiling

The Convention 108+ framework specifies that the right to challenge decisions arrived at through automated decision-making processes must include the opportunity to point out inaccuracies in personal data before it is used, the irrelevance of the profile being used to the data subject's particular case, or any other factors that would have an impact on the eventual decision. It also equips data subjects with the right to know the reasoning behind the decisions arrived at through automated processes, and the consequences of such reasoning.⁴⁴⁵ This is so that the data subject is able to meaningfully exercise other rights and make use of safeguards, such as the right to object or complain to the relevant data protection authority.

The GDPR also specifies that decisions based solely on automated processing cannot be based on special categories of personal data, such as data revealing racial or ethnic origin, religious beliefs, or biometric information).⁴⁴⁶ However, this restriction would not apply if the data subject explicitly consents to the processing and is not prevented by law from providing such consent, or it is necessary for substantial public interest and based on a law with adequate safeguards.⁴⁴⁷ It also requires controllers to undertake data protection impact assessments (DPIAs) in case of "a systematic and extensive evaluation of personal aspects relating to natural persons" based on automated processing, and where personal data is processed for special categories of data.⁴⁴⁸

While this right applies to private entities and actions taken by them, it can be especially important in the context of state action, especially when it pertains

to receiving social or financial benefits.⁴⁴⁹ While the right against automated decision-making seeks to increase accountability and safeguard data subject rights, the extent to which this occurs will depend on how it is implemented. More generally, concerns have also been raised about the technical difficulties with exercising this right (such as explaining the workings of complex "black box" machine learning systems) in terms of how they will vary based on the interpretation of the provision,⁴⁵⁰ though there is some guidance on how this provision would apply.⁴⁵¹

5.6.1.1 Exemptions to the right against automated decision-making and profiling

The GDPR and Convention 108+ limit a data subject's ability to exercise the right against automated decision-making, if the processing is authorised by a law which lays down suitable safeguards to protect the rights and interests of data subjects.⁴⁵² The GDPR details some of the safeguards meant to protect data subjects in that it specifies that even when such processing is allowed by law, the safeguards provided must include: (i) providing specific information on the automated processing and decision to the data subject and the right to obtain human intervention; (ii) to express their views to the controller on the decision arrived at by the automated processing; (iii) obtain an explanation of the decision that has been arrived at, and (iv) to challenge the decision arrived at through automated decision-making.⁴⁵³ It also specifies that such measures must not concern children, and requires controllers to implement relevant measures to ensure that inaccuracies in data are corrected and risk of errors are minimised, data is secured to account for potential risks to the rights of data subjects, and that discriminatory effects to data subjects on the basis of special categories of data are prevented.

445 Convention 108+, art 9(1)(c); Explanatory Report – Convention 108+, [75, 77].

446 GDPR, art 9(1).

447 GDPR, art 22(4).

448 GDPR, art 35(3).

449 Explanatory Report – Convention 108+, paras 75, 77.

450 For example, see Sandra Wachter, Brent Mittelstadt, and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' [2018] 31(2) Harv J of Law and Tech 841, 860-861, 873-874, 876-877, and 880-881.

451 UK Information Commissioner's Office, 'What else do we need to consider if Article 22 applies?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/>; Explanatory Report – Convention 108+, para 77.

452 Explanatory Report – Convention 108+, [75]; GDPR, art 22.

453 GDPR, recital 71.

Box 5.1: The Law Enforcement Directive

The Law Enforcement Directive ('LED') is legislation passed alongside the GDPR that deals with the processing of personal data for 'law enforcement purposes' (which falls outside the scope of the GDPR).⁴⁵⁴ It covers processing by "competent bodies" for "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".⁴⁵⁵ In this context, a 'competent body' would include not only public authorities, but also any other bodies entrusted by law to exercise public authority for the purposes specified above.⁴⁵⁶ The LED provides rights to data subjects and contains obligations for competent bodies. It also prohibits automated decision making unless authorised by laws with appropriate safeguards, and prohibits profiling that results in discrimination on the basis of special categories of personal data such as religious beliefs, genetic data, biometric information, etc.⁴⁵⁷ The LED also contains provisions relating to cross-border data transfers (as explored in Chapter 8 on the Regulation of Cross-Border Data Flows.)

5.7 The right to delegate (or for third-party to exercise) rights

The HIPCAR Privacy Framework specifically allows third parties to exercise rights on behalf of the data subject in certain circumstances, such as where the data subject is a minor, in the case of death, under a power of attorney, or by the data subject's guardian.⁴⁵⁸ Although additional details are not provided, this could be relevant in the context of legal heirs or

representatives being able to make some decisions on behalf of data subjects, and for information related to minors provided to the government. The OAS Principles also allow third parties to exercise the right of access on behalf of a data subject – for instance, parents on behalf of minor children.⁴⁵⁹

454 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [Law Enforcement Directive], available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>.

455 Art 1, Law Enforcement Directive.

456 Art 3(7), Law Enforcement Directive.

457 Art 11(1-3), Law Enforcement Directive.

458 HIPCAR Model Legislative Text, s 25.

459 OAS Principles with Annotations, Principle 8, page 18.

5.8 Whistle-blower protection

Interestingly, the HIPCAR Privacy Framework also contains a provision that protects whistle-blowers. While this is not a data-subject right per se, it is aimed at holding employers accountable. This provision specifies that employers, including public authorities, “shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee a benefit” because the employee undertook actions relating to preventing or notifying contraventions of the framework.⁴⁶⁰ Provisions aimed at protecting whistle-blowers can help increase accountability and ensure the effective implementation of data protection frameworks.



⁴⁶⁰ HIPCAR Model Legislative Text, s 78.

5.9 General exceptions to rights of data subjects

While some specific limitations to data subject rights have been discussed through the chapter, all Identified Regional Frameworks also contain general exceptions to the rights of data subjects and the obligations of data controllers. These exemptions are usually only applicable pursuant to laws which specify adequate safeguards and are required for purposes such as national security and protecting freedom of expression. The exceptions vary based on the framework in question, and some are broader than others. Importantly, such restrictions must be provided by law and proportional to the aims sought to be achieved. These elements have been discussed in detail in Chapter 7 (Government Access).

The HIPCAR Privacy Framework and the Commonwealth PPI Bill contain additional exemptions. The HIPCAR Privacy Framework exempts compliance with controller obligations and data subject rights under the framework processing for discharging functions relating to regulatory activities pursuant to law, to the extent that the application of the framework would likely prejudice the discharge of its functions. It also exempts compliance with controller obligations and data subject rights under the framework data processing for publication of journalistic, literary, or artistic material, where the controller believes it would be in the public interest especially as regards the freedom of expression, and that compliance with the framework would be incompatible with the relevant purpose. The Data Commissioner is allowed to establish codes of conduct in this regard, to balance the rights protected under the framework with the freedom of expression.⁴⁶¹ Similarly, the Commonwealth PPI Bill also exempts processing for solely journalistic, artistic, or literary purposes.⁴⁶²

5.9.1 Disclosure of exemptions to the rights of data subjects

Some frameworks specifically require states to disclose any restrictions to the rights of data subjects, which are essential to maintain transparency and accountability. The OECD Guidelines require that exceptions to the guidelines should be as few as possible and be made known to the public, and requires Member States to limit exceptions to those necessary in a democratic society.⁴⁶³ Similarly, the APEC Privacy Framework requires all exceptions to be limited and proportional to the intended objectives, and be disclosed publicly or be in accordance with law.⁴⁶⁴

The OAS Principles specifically require national authorities to publicly disclose any exceptions made to the Principles, and stress the importance of narrowly tailoring such exceptions and balancing competing interests.⁴⁶⁵

461 HIPCAR Model Legislative Text, ss 36, 37.

462 Commonwealth PPI Bill, s 5(2)(c).

463 OECD Privacy Guidelines 2013, para 4; Original Explanatory Memorandum OECD Guidelines, 53 and 54.

464 APEC Privacy Framework, para 18.

465 OAS Principles with Annotations, Principle 12, page 27.

Key considerations

- ◇ The rights of data subjects are an essential part of data protection frameworks and enable data subjects to operationalise various aspects of the right to privacy. The right of data subjects to access information that a controller has on them serves as the basis for all other rights, and is closely linked to the principles of transparency and accountability. The right to rectification can serve to reduce exclusions and bias, especially where personal data processing is the basis of public and financial services.
- ◇ Similarly, the right against automated decision-making enables data subjects to contest unfair or exclusionary decisions made purely on the basis of automated processing. The right to object can also help prevent harm to data subjects by enabling them to prevent controllers from processing their data, especially where it relates to direct marketing or where they are being subject to substantial harm as a result of the processing.
- ◇ The right to be forgotten can enable individuals to overcome stigma and judgment arising from past experiences, but must be balanced against very real threats to the access to information and the right to speech.
- ◇ The right to data portability provides data subjects with more control over their data and can enable interoperability and increased competition. The rights to restrict processing, to delegate the exercise of rights, and provisions such as whistle-blower protections serve to enable data subjects to effectively exercise the other rights available to them.

“ The rights of data subjects are an essential part of data protection frameworks and enable data subjects to operationalise various aspects of the right to privacy.... ”

CHAPTER 6

SPECIAL PROTECTIONS FOR CHILDREN'S DATA



6.1 Introduction

This chapter will discuss important factors that should be considered in international debates on data protection and privacy regulation while exploring the existing and potential harms that children face online. Based on international, regional, and domestic frameworks, this chapter will also analyse certain policy themes and recommendations on how to better address the protection of children's privacy embedded within the United Nations Convention on the Rights of the Child (CRC).

Even prior to the global COVID-19 pandemic, innovative technologies offered several benefits for both adults and children. As the world grappled with containing and managing the deadly pandemic, however, the virtual environment has gained significant attention as it features a 'new normal'. This has been characterised by a surge of information flows coupled with an increased reliance on technology and digital tools to carry out day-to-day activities, such as working-from-home, e-learning, and tele-health.⁴⁶⁶ Despite the internet being a powerful tool that has facilitated various aspects of human life during these unprecedented times, it has also exposed adults and children to new, unknown challenges. This is especially true from the perspective of informational privacy, data protection, and online safety.⁴⁶⁷

While many of these challenges over protection of data have largely been discussed in the context of adults, such technologies also have adverse repercussions on the lives of children and leave the

way open for potential harm. This can be largely attributed to children's lack of agency over their personal data, as well as technology that is typically not designed considering children's rights and their varied developmental levels. Therefore, concerns relating to the use of children's personal data as well as the protection of their privacy are unique and require special attention.⁴⁶⁸

Given that both the state and private organisations collect the personal data of children, often in the absence of adequate data protection frameworks and legal safeguards tailored to children, this gives rise to privacy risks and related harms. For example, schools across Russia have now installed cameras to monitor children on campus, and identify strangers who attempt to enter school grounds, in an effort to decrease the crime rates prevalent in Russian schools.⁴⁶⁹ Similarly, government-funded schools in India's capital city, Delhi, have installed facial recognition technologies as well as closed circuit

466 Yan Xiao and Ziyang Fan, '10 technology trends to watch in the COVID-19 pandemic' (World Economic Forum, 27 April 2020) <https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth/>.

467 Steven Vosloo, Melanie Penagos and Linda Raftree, 'COVID-19 and children's digital privacy' (UNICEF, 7 April 2020) <https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy>.

468 Andrew Young, Stuart Campo and Stefaan G. Verhulst, 'Responsible Data For Children' (UNICEF 2019) p 2 <https://rd4c.org/assets/rd4c-synthesis-report.pdf>.

469 Matthew Luxmoore, 'Yes, Big Brother IS Watching: Russian Schools Getting Surveillance Systems Called "Orwell"', (Radio Free Europe/Radio Liberty, 17 June 2020) <https://www.rferl.org/a/russian-schools-getting-surveillance-systems-called-orwell-/30676184.html>.

television cameras to ensure the safety of students.⁴⁷⁰

In the context of government-to-citizen services, the use of ICT has increased multi-fold over the years. The 2020 UN E-Government Development Index indicates that about 80% of the 193 UN Member States currently provide digital services for youth, women, older people, persons with disabilities, migrants, and those living in poverty.⁴⁷¹ E-government services are also being made available to children to improve accessibility to resources such as education, social services, and health care. Such services are largely provided by governments to children through the digitisation of their identities.

Ghana, for example, has recently introduced the Ghana Digital Card, through which citizens aged 15 and over will have a digital legal identity certification that allows them to access public and commercial services.⁴⁷² In the Philippines, the registration process indicates that children below the age of 5 can receive a PhilID upon registration, where their demographic information, biometric data and photograph are collected.⁴⁷³ India, similarly allows for children below the age of 5 to receive an Aadhaar number. There is no collection of biometrics, however, until the age of 5; demographic information and a facial photograph is collected at the time of enrolment.⁴⁷⁴ While instituting identification management for children in order to access digital services is intended to create a more inclusive system for integration and governance, countries worldwide have faced several challenges in ensuring the protection of children's data within such systems.⁴⁷⁵

As mentioned earlier, reliance on technological tools has grown as a result of the pandemic. These tools have been used to combat the effects of the pandemic and address public health concerns, causing an increase in the collection of personal data of both adults and children. Measures that gained attention and use during the COVID-19 pandemic such as contact tracing, for instance, have allowed for the interactions of children to be monitored and collected.⁴⁷⁶ In light of the use of such technological solutions to address challenges brought by the pandemic, UNICEF's Responsible Data for Children initiative highlights that further harms can arise out of the identification of children's data. Special considerations for the protection of children's personal information, however, has not received sufficient attention from states throughout the ongoing pandemic.

A few existing legal frameworks such as the GDPR do afford protections to children's data. These frameworks also provide exceptions to processing of personal data during a public health crisis. This may partly explain the lack of adequate focus on children's personal information during the pandemic.⁴⁷⁷ These circumstances, nonetheless, continue to highlight the existing need for effective consideration of the protection of children's data within data protection frameworks.

In the absence of legal and regulatory frameworks that specifically carve out safeguards for the protection of children's personal data, their right to privacy may be at risk owing to unchecked data collection and processing practices.

470 Rina Chandran, 'Fears for children's privacy as Delhi schools install facial recognition', (Reuters, 2 March 2021,) <https://www.reuters.com/article/us-india-tech-facialrecognition-trfn/fears-for-childrens-privacy-as-delhi-schools-install-facial-recognition-idUSKBN2AU0P5>.

471 United Nations Department of Economic and Social Affairs, 'E-Government Survey' (United Nations Department of Economic and Social Affairs, 10 July 2020) p xxv <https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey>.

472 Ghana National Identification Authority, 'Synopsis of the National Identification System Project' (29 May 2018) <https://nia.gov.gh/2018/05/29/synopsis-of-the-national-identification-system-project/>.

473 'Frequently Asked Questions' (Philippine Identification System, 2021) <https://www.philsys.gov.ph/faq/>.

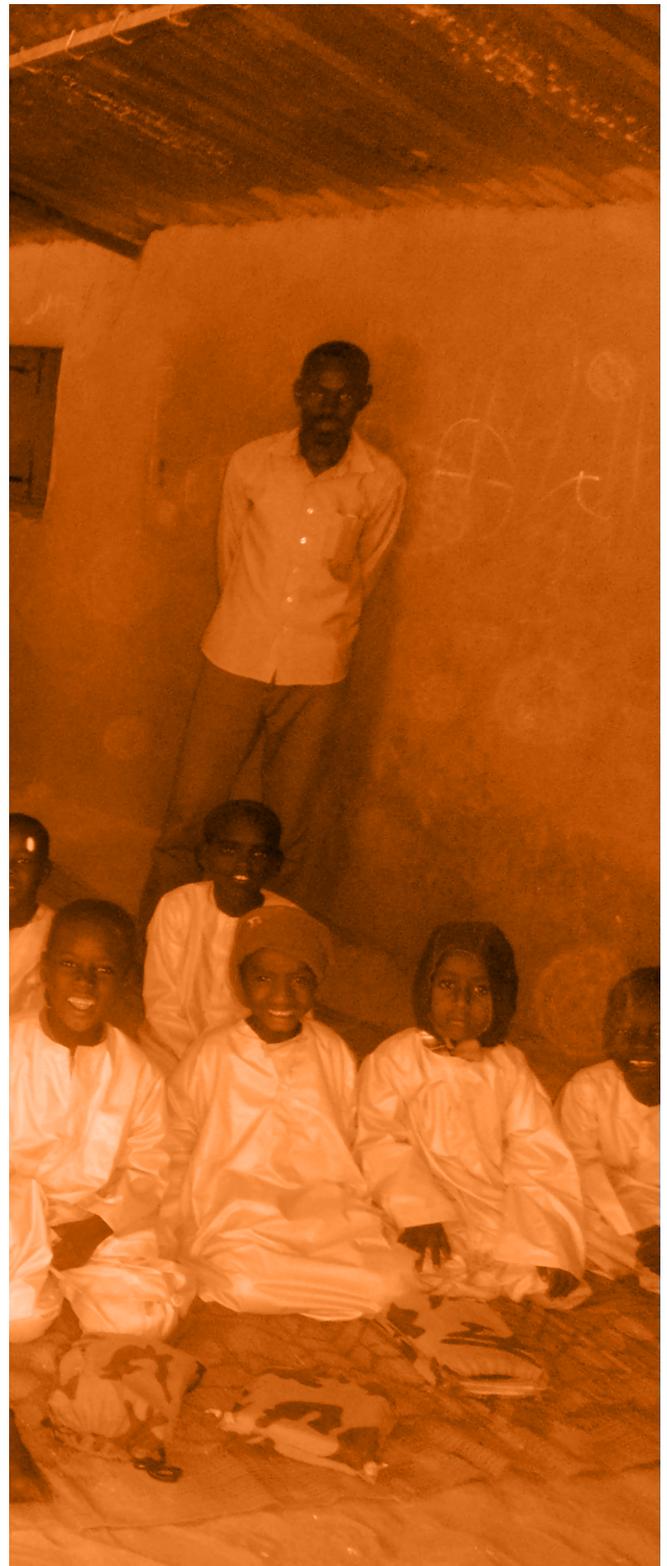
474 'FAQs: Enrolling Children' (Unique Identification Authority of India, 2021) <https://uidai.gov.in/contact-support/have-any-question/299-faqs/enrolment-update/enrolling-children.html>.

475 Zoë Pelter and others, 'Government Digital Services And Children: Pathways To Digital Transformation' (UNICEF 2021) p 13-15 https://www.unicef.org/globalinsight/media/1481/file/UNICEF-Global-Insight_e-gov-services-rapid-analysis-2021.pdf.

476 Steven Vosloo, Melanie Penagos and Linda Raftree, 'COVID-19 and children's digital privacy' <https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy>.

477 Linda Raftree, Emma Day and Jasmina Byrne, 'COVID-19: A Spotlight On Child Data Governance Gaps' (UNICEF 2020) p 2 <https://www.unicef.org/globalinsight/media/1111/file/UNICEF-Global-Insight-data-governance-covid-issue-brief-2020.pdf>.

As education moves online, the growth of education technology, or 'edtech', in schools has similarly resulted in increased rates of collection, sharing, and storage of children's personal data. Such information includes names, home addresses, and email IDs that has, in turn, enabled intrusive surveillance or the collection of information on children without parental consent.⁴⁷⁸ Though the COVID-19 pandemic calls for emergency measures to ensure continuity in learning for children, governments, parents, schools, and teachers must keep the data protection rights of children at the forefront while planning online pedagogy. Such pedagogy must not only be inclusive but also least intrusive in context of data collection and privacy of children.



478 Hye Jung Han, 'As Schools Close Over Coronavirus, Protect Kids' Privacy in Online Learning' (Human Rights Watch, 2020) <https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning>.

6.2 Current international and regional regulatory frameworks on children's data

Child rights, including their right to privacy, are recognised widely by international frameworks such as Article 16 of the United Nations Convention on the Rights of the Child.⁴⁷⁹ Article 16 enshrines a child's right to freedom from arbitrary interference with their privacy and further provides that children have the right to the protection of the law against any such interference. All the rights enshrined in the CRC are interdependent and indivisible, and are to be implemented in accordance with six guiding principles, namely: non-discrimination; the best interests of the child; the right to survival and development; the right to be heard; the right to access; and the right to education and digital literacy.⁴⁸⁰

When the right to privacy is extended to the digital realm, incorporating these principles within data protection legal and regulatory frameworks, both regional and national, must consider a child rights-based approach. This must safeguard their privacy, mitigate risks such as discrimination, and act in their best interests. At the same time, such a framework should also uphold children's participatory and emancipatory rights that are necessary for them to develop autonomy.⁴⁸¹

Among the many international and regional legal and regulatory frameworks governing privacy and data protection, only the GDPR and the recently revised OAS Principles provide for child-specific consent in the digital context. In 2021, the annotations to the OAS Principles have been updated to include requirements that a data controller must obtain authorisation from a guardian or parent or directly

from the minor when the law requires a minor's consent without requiring parental/guardian representation.⁴⁸² While a 2018 resolution by the Council of Europe advised Member States to protect children in the digital environment from monitoring and surveillance carried out by state authorities and/or private sector entities, these recommendations are yet to be effectively implemented.⁴⁸³ In 2021, the United Nations Committee on the Rights of the Child also released a general comment on children's rights in the digital environment.⁴⁸⁴

479 Convention on the Rights of the Child (adopted 20 November 1989 UNGA Res 44/25, entered into force 2 September 1990) 1577 UNTS 3, art 16.

480 CRC, art 28, art 17, art 12, art 6, art 3, art 2; Jonathan Todres and Shani M. King, *The Oxford Handbook of Children's Right Law* (OUP 2020).

481 Soo Jee Lee, 'A Child's Voice Vs. A Parent's Control: Resolving A Tension Between The Convention On Rights Of The Child And U.S. Law' (2017) 117 *Columbia Law Review*.

482 OAS Principles with Annotations, Principle 2, p 10

483 Council of Europe, 'Recommendation CM/Rec (2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment' (Committee of Ministers, 1321st meeting of the Ministers' Deputies, 4 July 2018) CM/Rec (2018)7 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7.

484 General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25.

6.3 Factors and risks involved in protecting children's personal data and online privacy

In addition to risks such as cyberbullying, sexual exploitation and trafficking, and promotion of self-harm, emerging issues such as surveillance, identity fraud, and breaches of information security have made children vulnerable and susceptible to threats online.⁴⁸⁵ Such threats not only infringe on children's right to privacy, but also endanger their experiences online. In light of these risks and threats that pose new challenges to policymakers, parents, and children, the following section discusses various factors that should be considered while protecting children's personal data and their online privacy.

6.3.1 Age of digital consent for children

Several surveys have indicated a growth in the percentage of children as well as adolescents and young people who go online to pursue various activities, including but not limited to instant messaging, gaming, e-learning, hobbies, entertainment, and downloading music.⁴⁸⁶ Children not only access the internet to reap the benefits of digital products and services, but also to participate in online activities that include content creation and media consumption. Most data protection frameworks allow data controllers and processors to collect, process and use personal data of users or individuals through consent-based privacy management tools.⁴⁸⁷

International and regional frameworks impose an 'age of digital consent', which is the minimum age a user must be to provide consent before organisations can collect, process and store their data without parental

consent. This protection ensures both the autonomy of a child to make informed decisions about their online activities and to shield them from any possible harms and threats found online.⁴⁸⁸

This may not be the best approach for children, owing to their vulnerability and lack of technical sophistication to assess any invasion to their personal data or privacy (please refer to Chapter 3 on Data Protection Principles for more information on the scope of consent obtained from users under international and regional frameworks).

Many existing frameworks have imposed specific age thresholds for children's digital consent in order to limit the collection and processing of their data and protect the child's right to privacy. For example, the GDPR's Article 8 states that each Member State should set its own digital age of consent between 13 and 16, which refers to the age at which young people may sign up for online services such as social media without needing the explicit consent of their parent or guardian. Similarly, the Children's Online Privacy Protection Act (COPPA), which took effect in the United States in 2000, sets the age of digital consent at 13, and specifically lists the requirements and conditions to be complied with by data controllers.⁴⁸⁹ Singapore's Personal Data Protection Act does not contain specific provisions with regards to children's data. The Personal Data Protection Commission, however, provides some guiding commentary. It observes that organisations, while determining if a minor can consent, should consider if they have "sufficient understanding of the nature and

485 'PISA 2015 Results (Volume III): Students' Well-being' (OECD 2017) https://www.oecd-ilibrary.org/education/pisa-2015-results-volume-iii_9789264273856-en; General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25, paragraph 16, page 3.

486 "Being Young in Europe Today - Digital World" (Eurostat: Statistics Explained, 2020) https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Being_young_in_Europe_today_-_digital_world#A_digital_age_divide.

487 APEC Privacy Framework, Part III, principle V, para 26; ASEAN DP Framework, principle 6(a); Commonwealth PPI, s 8; GDPR, art 7; HIPCAR Model Legislative Text, s 9(1); OECD Guidelines, Part 2, principle 7; OAS Principles with Annotations, principle 2, p 1.

488 Liliana Pasquale and others, 'Digital Age Of Consent And Age Verification: Can They Protect Children?' [2020] IEEE Software (Early Access) <https://ieeexplore.ieee.org/document/9295422>.

489 Children's Online Privacy Protection Act of 1998, 15 USC 6501–6505 (COPPA), 16 CFR Part 312.

consequences of giving consent.”⁴⁹⁰ Recognising that some organisations already consider an age threshold of 13 as sufficient to require consent, the Commission states that, as a “practical rule of thumb”, it would similarly consider that a minor of 13 years has reached a consenting age.

Such thresholds have been imposed by drawing upon traditional age of consent models for various activities, such as entering into contracts, having sexual relations, and undergoing medical procedures. For example, in India, laws dealing with juvenile justice, evidence, and labour define child differently based on their age and maturity.⁴⁹¹ However, India's proposed data protection legislation imposes a blanket age threshold of 18 years for consent similar to the Indian Contract Act, 1872, which considers a minor to be any person below the age of 18 years, and subsequently declares all contracts entered into by minors as non-enforceable.⁴⁹² With regard to India's Aadhaar (biometric-based digital ID programme), a child's enrolment for Aadhaar can only be done with parental consent, and the legal framework has been amended to give minors the choice to opt out within six months of turning 18 years of age.⁴⁹³

Indonesia, like India, defines a child differently within its laws and regulations, depending on the purposes involved. For example, child welfare laws establish that an individual is deemed to be a child when under the age of 21. Meanwhile, the law defines a child as under the age of 18 for human rights and juvenile delinquency purposes.⁴⁹⁴

Experts agree that as children get older, their



understanding and experiences evolve to better understand the digital ecosystem. However, not all children behave and adapt in the same way.⁴⁹⁵ Children across various ages require different and specific online support, protection, and freedoms. Although differences in the age of children are likely to determine the degree of vulnerability or risk and resilience to online harms, the continued adoption of consent-based mechanisms by international and regional frameworks are proving to be inadequate. For instance, critics of the GDPR have raised several concerns relating to the consent mechanism for children under existing regulation, on the grounds that parental consent may not be sufficient to protect children in a digital world.⁴⁹⁶ Additionally, studies conducted by different organisations and regulatory bodies prescribe different ages for consent, thereby creating confusion and lack of uniformity.⁴⁹⁷ Without

490 Personal Data Protection Commission, 'Advisory Guidelines On The Personal Data Protection Act For Selected Topics' (Personal Data Protection Commission Singapore 2021) p 53-54.

491 Child Labour (Prohibition and Regulation) Act, 1986, s. 2(ii); Indian Evidence Act, 1872, s. 118; Juvenile Justice (Care and Protection of Children) Act, 2015, s. 15.

492 India, Indian Contract Act, 1972, s. 11; Report of the Joint Committee on the Personal Data Protection Bill, 2019, s 57(2)(d) available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.

493 Justice KS Puttaswamy v Union of India (2019) 1 SCC 1 [https://privacylibrary.ccglnud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uo-i-and-ors; India, Aadhaar And Other Laws \(Amendment\) Act, 2019, s 5](https://privacylibrary.ccglnud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uo-i-and-ors; India, Aadhaar And Other Laws (Amendment) Act, 2019, s 5).

494 Riduansyah and others, 'Children's Rights Conflict with The Law in The Time of The COVID-19 Pandemic' (2021) 10 International Journal of Criminology and Sociology 1156 <https://ns1.6thsigmahosting.com/pms/index.php/ijcs/article/view/8107>.

495 Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data And Privacy Online: Growing Up In A Digital Age' (LSE Media and Communications 2018) p 7 <<https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf>>.

496 Vicki Shotbolt, 'Is Parental Consent The Way Forward, Or Is The GDPR The End Of Young People's Freedom To Roam Digitally?' <<https://blogs.lse.ac.uk/mediase/2016/12/13/is-parental-consent-the-way-forward-or-is-the-gdpr-the-end-of-young-peoples-freedom-to-roam-digitally/>>; Milda Macenaite and Eleni Kosta, 'Consent For Processing Children's Personal Data In The EU: Following In US Footsteps?' (2017) 26 Information and Communications Technology Law 159, 160 <<https://www.tandfonline.com/doi/citedby/10.1080/13600834.2017.1321096?scroll=top&needAccess=true>>.

497 Sonia Livingstone and Kjartan Ólafsson, 'Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the GDPR' <<https://blogs.lse.ac.uk/mediase/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/>>.



a clear understanding and agreement on the varying ages of consent, an irregular prescription of such ages may add to data controllers' legal risks and compliance burdens.

Furthermore, obtaining and enforcing the requirement of providing 'meaningful' consent from children that is explicit, free, and specific is challenging for data controllers.⁴⁹⁸ Though some data controllers have created alternative versions of their products and services for children with limited features (such as YouTube Kids or Netflix Kids), there remains a risk that children will misrepresent their age in order to use versions of such products and services originally designed for adults, which would make them more vulnerable to privacy threats and security breaches.⁴⁹⁹ For consent verification mechanisms to be effective and easy, they should comply with the main data

protection principles, such as data minimisation, purpose limitation, data adequacy and relevance. Requiring more data for verification to 'protect' children increases the quantity of data collected and goes against the principle of data minimisation. Eventually, this may not result in serving the privacy interests of children.⁵⁰⁰

At the same time, regulatory frameworks, such as the UK ICO's Gillick competence test,⁵⁰¹ have acknowledged the evolving capacities of children who are capable of exercising agency over their online decisions.⁵⁰² A recent UNICEF Innocenti study demonstrates that while most older children know how to manage online privacy settings, only a few younger children report that they can do so. Therefore, setting an 'appropriate age' for digital consent must factor in the impact of emerging technologies on children's cyber cognitive development. It must also take into account whether they have adequate digital skills to understand the consequences of sharing their data, and are capable of exercising any digital rights arising from the misuse of any such data.⁵⁰³ While the UN defines a child as, "every human being below the age of 18 years, unless, under the law applicable to the child, majority is attained earlier,"⁵⁰⁴ it would be helpful to assess media literacy levels, legal traditions, and cultural contexts of children residing in different geographical regions to determine a suitable digital age of consent to better protect them according to their diverse backgrounds. Although 'age appropriate' can protect a child when customised, it may not be sufficient to protect a cohort of children of the same age who show varied intellectual and emotional development. Therefore, such inequity in developing

498 Milda Macenaite and Eleni Kosta, 'Consent For Processing Children's Personal Data In The EU: Following In US Footsteps?' (2017) 26 *Information and Communications Technology Law* 159, 160 <<https://www.tandfonline.com/doi/citedby/10.1080/13600834.2017.1321096?scroll=top&needAccess=true>>.

499 Mary Aiken, *The Cyber Effect: An Expert in Cyber Psychology Explains How Technology Is Shaping Our Children, Our Behavior, and Our Values - and What We Can Do About It*, (Penguin Random House 2017); danah boyd and others, 'Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'', (Berkman Klein Center, 2011) <<https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075>>.

500 OHCHR, 'Report of the Special Rapporteur on the Right to Privacy' (2021) UN Doc A/HRC/46/37 <https://undocs.org/A/HRC/46/37>; Lina Jasmontaite and Paul De Hert, 'The EU, Children Under 13 Years, And Parental Consent: A Human Rights Analysis Of New, Age-Based Bright-Line For The Protection Of Children On The Internet' (2015) 5 *International Data Privacy Law* 20-33 <https://academic.oup.com/idpl/article-abstract/5/1/20/2863826>.

501 'What Is Valid Consent?' (Information Commissioner's Office, 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent>.

502 General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25, paragraph 71, page 12.

503 Jasmina Byrne and others, 'Global Kids Online: Research Synthesis 2015-2016' (UNICEF, Office of Research-Innocenti and The London School of Economics and Political Science 2016) http://eprints.lse.ac.uk/67965/7/Global%20Kids%20Online_Synthesis%20report_2016.pdf.

504 CRC, art 1.

age appropriate measures for a child groups could potentially constrain development of children's personality, the autonomous exercise of their rights, and possibly also be discriminatory.⁵⁰⁵

6.3.2 The role of parental consent

As indicated above, policymakers have sometimes prescribed obtaining parental consent on behalf of children accessing the internet. This is due to children's lack of knowledge and understanding to make informed decisions for themselves.⁵⁰⁶ Many frameworks, including the GDPR, the OAS Principles, Malaysia's Personal Data Protection Act 2010, Ghana's Data Protection Act, COPPA, as well as India's proposed data protection legislation⁵⁰⁷ require parental consent for children within specific age groups to use digital products and services. Such parental consent has been required not only to empower children when they participate in digital transactions and content consumption to ensure decisions are made in the child's interest, but also to protect them from any potential harm.⁵⁰⁸ The requirement for parental consent is based on the premise that parents possess the maturity, experience, and capacity for judgment that children lack when making difficult decisions, and that they will act in the best interests of their offspring.⁵⁰⁹ However, the conflict between protective rights and children's participatory or emancipatory rights can be seen in most child rights' laws,⁵¹⁰ and can also be broadened to include the right to privacy. Since

these participatory or emancipatory rights include children's right to online decision-making and freedom of expression, requiring parental consent could be construed as contradictory to the CRC principles, which are based on the best interests of the child and their evolving capacities, participation, and right to self-determination.⁵¹¹ It is worth noting that there are some legal and regulatory frameworks that allow children to provide consent when they attain a specific age. However, these frameworks may not adequately consider the sociological, psychological, and other relevant factors when determining their understanding of the digital space. At the same time, determining the age at which specific protections for children should be lowered, based on their level of maturity, is a challenge, as some children at a particular age may not yet be competent to take responsibility for their online decisions.

Further, parental consent does not eliminate the privacy risks that both parents and children might not be cognisant of or further those risks they may continue to face. A 2016 World Health Organization (WHO) report regarding online food advertisements targeting children concluded that parents were unaware of both the profiling techniques used to target children, and the related risks.⁵¹² In addition, while parental consent may to some extent protect children from data processing undertaken by private companies and the state and promise operational ease, it does not factor in any threats to children's privacy by parents. Furthermore, adults may not

505 'The Case For Better Governance Of Children's Data: A Manifesto' (UNICEF 2021) <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>; Information Commissioner's Office, 'Age Appropriate Design: A Code Of Practice For Online Services' (2020).<https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>.

506 'Children and the UK GDPR' (Information Commissioner's Office) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/>; General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25, paragraph 71, page 12.

507 India, Report of the Joint Committee on the Personal Data Protection Bill, 2019 available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf; COPPA, 15 USC 6501–6505; Ghana, Data Protection Act, 2012; Malaysia, Personal Data Protection Act, 2010; General Data Protection Regulation (EU) 2016/679 OJ L119/1.

508 Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data And Privacy Online: Growing Up In A Digital Age' (LSE Media and Communications 2018) <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf>.

509 CRC, art 3, para 1; United Nations High Commissioner for Refugees, 'Guidelines on Determining the Best Interests of the Child' (UNCHR, 2008) <https://www.unhcr.org/4566b16b2.pdf>.

510 Soo Jee Lee, 'A Child's Voice Vs. A Parent's Control: Resolving A Tension Between The Convention On Rights Of The Child And U.S. Law' (2017) 117 Columbia Law Review..

511 CRC, art 16.

512 Dr Mimi Tatlow-Golden and others, 'Tackling food marketing to children in a digital world: trans-disciplinary perspectives' (World Health Organization, 2016) https://www.euro.who.int/__data/assets/pdf_file/0017/322226/Tackling-food-marketing-children-digital-world-trans-disciplinary-perspectives-en.pdf.

always be able to understand the complex interactions between information technology and children.⁵¹³

Prioritisation of parental consent and subordination of children's privacy runs contrary to well-established principles in international law, which state that children need special legal protection, and courts must give primary consideration to their best interests in decisions affecting their lives.⁵¹⁴ Such protection cannot be solely contingent upon the consent, wishes or behaviour of a parent who, in turn, might override children's rights to freedom of expression and digital participation.⁵¹⁵

In this regard, COPPA adopts a risk-based approach by not requiring parental consent for commercial services that do not share children's personal data or are not interactive. The risk-based approach here would relate to the extent of data collection and the consequential risk to the child. For instance, services that are not interactive involve very limited collection of children's data to perform one-time requests for a specific purpose such as collecting a child's contact information to enter into a contest.⁵¹⁶ In such circumstances, COPPA necessitates that information collected cannot be shared or even maintained after the request is complete to protect against misuse. Similarly, the UK government, in addition to compliance with the GDPR and the UK's Privacy and Electronic Communications Regulations, has taken a risk-based approach and set out standards of age appropriate design for online services in its Age-Appropriate Design Code of Practice (Children's Code).⁵¹⁷ The Children's Code consists of technology-neutral design principles and practical privacy features, such as data minimisation and data protection impact

assessments. These are to be implemented by all data controllers that offer online services likely to be used by children, including social networking and applications, connected toys, video game platforms, streaming services and educational websites. Critics have raised concerns, that in an attempt to distinguish children as users online, to afford specific protections, the Children's Code might lead to the increased collection of children's personal data. This can arise in trying to create the distinction, and use this to further child engagement.⁵¹⁸ This would, in turn, require more restrictions on behavioural advertising and data processing which would require the need for higher default privacy settings for children of younger ages.

There is a growing need for legal and social frameworks to adequately accommodate the widely varying capacities of children over different aspects of their lives, and enable them to provide consent in their individual capacities.⁵¹⁹ In order to balance the participatory and emancipatory rights of children vis-a-vis their right to privacy, the presence of parental consent, to the extent possible, may be taken into account to establish consent for limited purposes (e.g. high value transactions), and to assess potential risks. It should not, however, elevate this factor above all others. To help in actualising this, a 'sliding-scale' approach for consent could be adopted to ensure that children are able to access the internet as an educational and functional tool to carry out activities for research or homework assistance.⁵²⁰ However, activities that could pose a greater risk to children could require parental consent to ensure that the collection of children's personal information by data controllers is legitimate and proportional to the purposes of use.

513 Danah Boyd, 'It's Complicated: The Social Lives of Networked Teens' (Yale University Press, 2015)

514 Jelena Gligrojevic, 'Children's Privacy: The Role Of Parental Control And Consent' (2021) 19 Human Rights Law Review <https://academic.oup.com/hrlr/article/19/2/201/5522387?login=true>.

515 'The Case For Better Governance Of Children's Data: A Manifesto' (UNICEF 2021) <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>.

516 Federal Trade Commission, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' (June 2017) <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#chart>.

517 Ariel Fox Johnson, 'Reconciling the Age-Appropriate Design Code with COPPA' (IAPP, 2021) <https://iapp.org/news/a/reconciling-the-age-appropriate-design-code-with-coppa/>; Information Commissioner's Office, 'Age Appropriate Design: A Code Of Practice For Online Services' (2020) <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>.

518 Matthew Rice, 'Age-Appropriate Design Code' (Open Rights Group, 2018) <https://www.openrightsgroup.org/publications/age-appropriate-design-code-consultation/>.

519 Gerison Lansdown, 'Can You Hear Me? The Right Of Young Children To Participate In Decisions Affecting Them' (Bernard Van Leer Foundation 2005) <https://bibalex.org/baifa/Attachment/Documents/114976.pdf>.

520 Lauren A. Matecki, 'Update: COPPA Is Ineffective Legislation! Next Steps For Protecting Youth Privacy Rights In The Social Networking Era' (2010) 5 Northwestern Journal of Law and Social Policy page 369, 400 <http://scholarlycommons.law.northwestern.edu/njls/vol5/iss2/7>; COPPA, 16 CFR Part 312.

“The state’s use of biometrics and other recent technological innovations that collect intimate information about individual has renewed interest to protect children who provide their personal data online”

Alternatively, as a substitute to requiring parental consent in any manner, a ‘balancing test’ can be applied whereby the degree to which data controllers will be permitted to share a user’s personal information would relate to the user’s age. Children under the age of 13, for example, would have mandatory ‘opt-in’ policies on data collection and processing, with none of their personal information shared without explicit consent. Meanwhile, users over 13 would have default ‘opt-out’ policies unless expressly refused. Such measures could potentially protect children’s best interests.

6.3.3 Age Verification techniques

The state’s use of biometrics and other recent technological innovations that collect intimate information about individual has renewed interest to protect children who provide their personal data online.⁵²¹ Given that such information is highly sensitive, online service providers, industry associations, and policymakers are taking steps to implement measures to verify the age of children who use digital products or services that may be potentially harmful. Such verification measures include those that require a child to simply declare their age or submit formal identity documents. Other measures involve relying on verifying a parent’s identity to ensure purposeful and meaningful consent is provided, or estimating the age of the child through behavioural analytics or facial scans.⁵²²

Modern verification techniques increasingly rely on the collection of additional data points, some of which have been pointed out in Chapter 1 (Introduction), such as proof of identity through digital IDs, live images of the individual or even the use of facial recognition software. However, this step forward may also run into concerns of excessive data collection and inaccuracy, amongst other potential risks. As a result, these concerns have necessitated stronger data protection laws. In light of these challenges, it is important to note that different levels of technological complexity within verification techniques need to be dependent on context and appropriateness of use, a consideration that is intensified when considering children’s data. While opening a bank account,

521 OHCHR, ‘Draft Legal Instrument on Government-led Surveillance and Privacy 16 Including the Explanatory Memorandum 17 Ver 0.6’, (2018) <https://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf>.

522 Emma Day, ‘Digital Age Assurance Tools and Children’s Rights Online across the Globe: A Discussion Paper’ (UNICEF 2021) <https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf>.

for example, a bank may require the provision of different forms of identification and advanced means of verification to comply with possible know-your-customer (KYC) or anti-money-laundering (AML) legal requirements. Similar identification techniques, such as verification of ID cards or the use of facial recognition technology, may be considered excessive when providing verification to register for a social media account. Therefore, the application of such verification systems may need to be cautiously considered with regards to age-verification measures for children.

While age-verification mechanisms may add an additional layer of safety for children online, it must be recognised that they are not fool-proof, and involve many challenges and opportunities. More importantly, given that age verification requires children to furnish personal information, such as date of birth, the sharing of children's personal data online may in fact intrude on their privacy and put them at greater risk when the data collection is not proportionate to the objective of such collection.

Online verification of identity, as a result, may be difficult to undertake and prone to misuse with inauthentic users presenting themselves as adults. An obligation could be placed on the data controller to implement user identity verification based on public datasets (e.g., social security number, driver's license, credit history, electoral roll) This could be done while enabling an audit trail for any regulatory oversight and compliance with regulations that require age verification. However, the same could be challenging, owing to a reliance on public datasets.

In some countries, the non-alignment of existing ID issuance authorities and birth registration authorities for children in rural areas has allowed for ID gaps or duplication, resulting in poor integration of children within the ID system.⁵²³ Such roadblocks could potentially disable children from accessing essential digital tools and services that require age verification based on existing digital and real IDs.

Given the lack of a unified legal framework or policy guidance in this regard, appropriate age verification strategies that may require simple self-reporting of age and date of birth are not used by data controllers to ensure adherence with the law. Even when used if inadequate mechanisms are deployed, it may, in fact, facilitate circumvention of rules.⁵²⁴ Age verification is rarely properly carried out in online settings, in comparison to offline situations, such as when a liquor store owner or casino manager may request patrons to furnish proof of ID to corroborate age and identity information. With an 'age gate', users accessing digital products and services are often asked to provide their date of birth, or otherwise state their age, before entering an age-restricted site or purchasing online products, such as alcohol or tobacco. While some controllers offering digital services take limited steps to verify the information provided by the user, such age-gating mechanisms act as the only barrier to content or product purchases that have legal age-based restrictions or limitations. However, such mechanisms may not be sufficient to safeguard against either the illegal purchase of age-restricted goods or services or limit exposure to age-rated advertising. The UK's Digital Economy Act, 2017, for example, requires that any commercially available pornographic material should not be "normally accessible to persons under the age of 18."⁵²⁵ Nevertheless, enforcement of such age-verification mechanisms may be limited.

In 2013, the UK's Office of Communications (OfCom) fined Playboy £100,000 for not implementing adequate age-verification controls to distinguish between credit and debit card purchases on its website, which offers users pornographic content. Given that debit cards can be issued to individuals under age 18, website pornographic content could be accessed by children and adolescents by entering their debit card numbers. OfCom stated that neither age self-verification nor debit card information are valid forms of age verification, and held Playboy liable for failing to protect children online. Playboy avoided the penalty as the payment was processed overseas, however, which was outside OfCom's limited jurisdiction.⁵²⁶

523 Zoë Pelter and others, 'Government Digital Services And Children: Pathways To Digital Transformation' (UNICEF 2021) https://www.unicef.org/globalinsight/media/1481/file/UNICEF-Global-Insight_e-gov-services-rapid-analysis-2021.pdf.

524 Dr Victoria Nash and others., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry', (Oxford Internet Institute 2012-2013) 21 <https://www.oii.ox.ac.uk/research/projects/effective-age-verification-techniques>.

525 United Kingdom, Digital Economy Act 2017, s 14.

526 Mark Sweney, 'Playboy Fined £100,000 For Offering Porn On Websites Accessible To Children' The Guardian (2013) <https://www.theguardian.com/media/2013/jan/16/playboy-fined-porn-accessible-children>.



As previously mentioned, children misrepresenting their age is fairly common, with approximately 39 percent of American teenagers, according to one study, falsifying their age in order to access restricted content and services.⁵²⁷ Another EU-backed study has shown how easy it is for children to misrepresent their age and bypass the most popular applications for age verification.⁵²⁸ As a consequence, there is a need to incentivise users to be honest and input their exact age. If it is determined that a user has provided incorrect information relating to their age, data controllers, for example, should consider means to prevent an individual from installing an application on a device which they have previously registered as an underage user.

Age-verification comes with several technical, operational, and legal challenges. Nevertheless, verifying a user's age and identity does foster trust that children are protected online from age-restricted products, services or content that may be harmful to them.⁵²⁹ It also provides a safer online environment where the freedom of speech and expression of a child can be supported.

-
- 527 Mary Madden and others, 'Teens, Social Media, and Privacy' (Pew Research Center, 2013) <https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/>.
- 528 Liliana Pasquale and others, 'Digital Age Of Consent And Age Verification: Can They Protect Children?' [2020] IEEE Software (Early Access) <https://ieeexplore.ieee.org/document/9295422>.
- 529 Emma Day, 'Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper' (UNICEF 2021) <https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf>.

Key considerations

While researchers and policymakers have studied the impact of emerging technologies on adults, there is limited research analysing how children and adolescents interact with new technologies. Literature on how to empower children in the digital world is also scarce. To address this gap of knowledge, and better understand existing challenges, it is critical to bring on board experts from diverse fields, including sociology, psychology, technology, law, and communications. The focus of such an approach should account for the cognitive vulnerabilities of young children of

different ages, living in diverse cultural contexts and from varying socioeconomic backgrounds. This is especially important when developing regulations that target children's privacy management and that determines the exact accountability of data controllers who process children's personal information. In light of the growing online presence of children, through the following mechanisms, children's data protection within legal frameworks can receive greater attention:

6.4.1 The importance of data minimisation

As more countries and regions adopt new privacy and data protection frameworks in tune with evolving technologies, high standards of privacy by design and default are required of data controllers.⁵³⁰ These requirements can ensure maximum compliance, privacy protection, and data security by collecting only the data that is required for the said product, service, or content.⁵³¹ Specific measures for data minimisation can be similarly considered in approaching children's data. By default, such frameworks should mandate limited collection and use of personal data of children by data controllers and processors to the extent that such data is essential for the provision of the service. Any use of personal data that is intrusive should be specifically and individually 'opted in' by the child or parent as applicable. For example, Standard 7 of the UK's Children's Code prohibits the collection

of more personal data than required to provide a service to a child.⁵³² To operationalise this provision, data controllers and processors could be required to differentiate between each individual element of their services in order to determine which personal information may be required for a child to access a required service. Data controllers should further ensure that mechanisms implemented facilitate the empowerment of children online. This can be done by offering them the right tools to exercise their data protection rights, such as: checking the accuracy of data shared or requesting the deletion of existing data; and informing them in a transparent manner about potential risks or harm resulting from data collection and processing.⁵³³ A general comment by the United Nations Committee on Right of the Child specifies that information provided to parents/caregivers and children related to data storage and processing must be done in a child friendly manner and in accessible formats.⁵³⁴

530 General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25, paragraph 70, page 12.

531 Pedro Hartung, 'The children's rights-by-design standard for data use by tech companies' (UNICEF, 2020) <https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf>.

532 Information Commissioner's Office, 'Age Appropriate Design: A Code Of Practice For Online Services' (2020).<https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>.

533 Council of Europe, 'Recommendation CM/Rec (2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment' (Committee of Ministers, 1321st meeting of the Ministers' Deputies, 4 July 2018) CM/Rec (2018)7 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7.

534 General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021) CRC/C/GC/25, paragraph 72, page 12.

6.4.2 Beyond age verification

Some websites and applications, such as those selling alcohol, require users to input their date of birth to verify their current age or ask for parental verification of such information. Legal frameworks, therefore, should necessitate that every user explicitly opts-in and verifies their age to access age-restricted products, services or content and to afford children a basic level of protection.

The UK Government's Communications Headquarters, along with the Department for Digital, Culture, Media and Sport, studied the challenges involved in verifying children's online access and discovered the value of assessing the age of children beyond purely age verification measures.⁵³⁵ It observed that the current approach to age verification is simply to distinguish between adult and children instead of categorising age groups depending on their online needs. This process termed as 'age assurance' involves understanding potential risks a platform poses and establishing the likelihood of risk to a child accessing the platform. It then applies the appropriate methods of verification proportionate to the degree of risk involved.

It suggests several different methods to 'assure a child's age' online, which is dependent on the degree of confidence and certainty that the platform has in the accuracy of the age provided by the user. This confidence is closely linked to the risk that the platform poses to the child. The methods listed, such as: a simple age declaration; confirmation of age from a digital parent (where parental responsibilities are extended to other relevant individuals online), peer group or official sources; or authentication from a trusted online provider. These methods can be used individually or in combination with each other on a case-by-case basis.⁵³⁶

For example, it is necessary for the platform to have a moderate degree of confidence in the accuracy of the user's age in a situation where a platform recognises that there is some degree of risk that it poses to a

child. This means that a combination of methods of verification appropriate to this risk must be employed, such as requiring a user to declare their age followed by an automated age verification method using online behaviour – behavioural data from previous use, could be one of the ways to confirm the declaration. Furthermore, mechanisms to deter child users from installing an app on a device on which they have previously misrepresented their age can be one of the measures to verify the age of users of applications that may negatively impact users below certain age groups.

“Legal frameworks, therefore, should necessitate that every user explicitly opts-in and verifies their age to access age-restricted products, services or content”

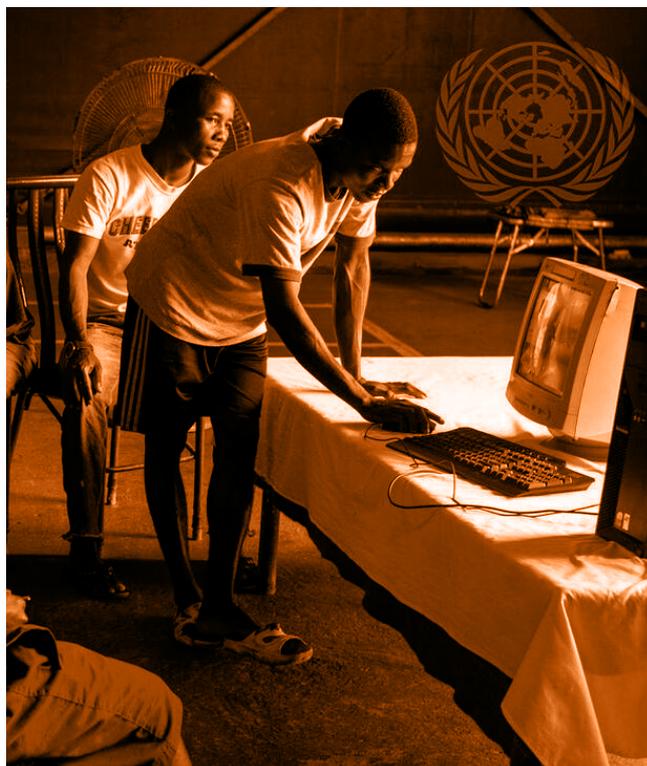
535 'VoCO (Verification Of Children Online) Phase 2 Report' (GCHQ, DCMS and the United Kingdom Home Office 2020) p 12, 13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934131/November_VoCO_report_V4__pdf.pdf.

536 'VoCO (Verification Of Children Online) Phase 2 Report' (GCHQ, DCMS and the United Kingdom Home Office 2020) p 18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934131/November_VoCO_report_V4__pdf.pdf.

6.4.3 Developing digital literacy

As more children and adolescents access online services, there is a growing need to equip them with the knowledge, resources, and tools that will assist them in understanding and assessing the potential risk or harm that digital products, services, and content may cause. The APEC Privacy Framework suggests that if organisations afford children with the option to consent to the collection and use of their data, information that is provided regarding the exercising of such choice must be done in a manner that is easily understandable and age appropriate.⁵³⁷ In 2020, a Convention 108 Consultative Committee introduced guidelines on Children's Data Protection in an Education Setting with recommendations aimed at legislators, policy makers, and data controllers to better protect and support children's rights with regards to the use of educational technology.⁵³⁸ For instance, the Guidelines point out that the deletion of profiles and history should be easy to carry out at the end of a session.

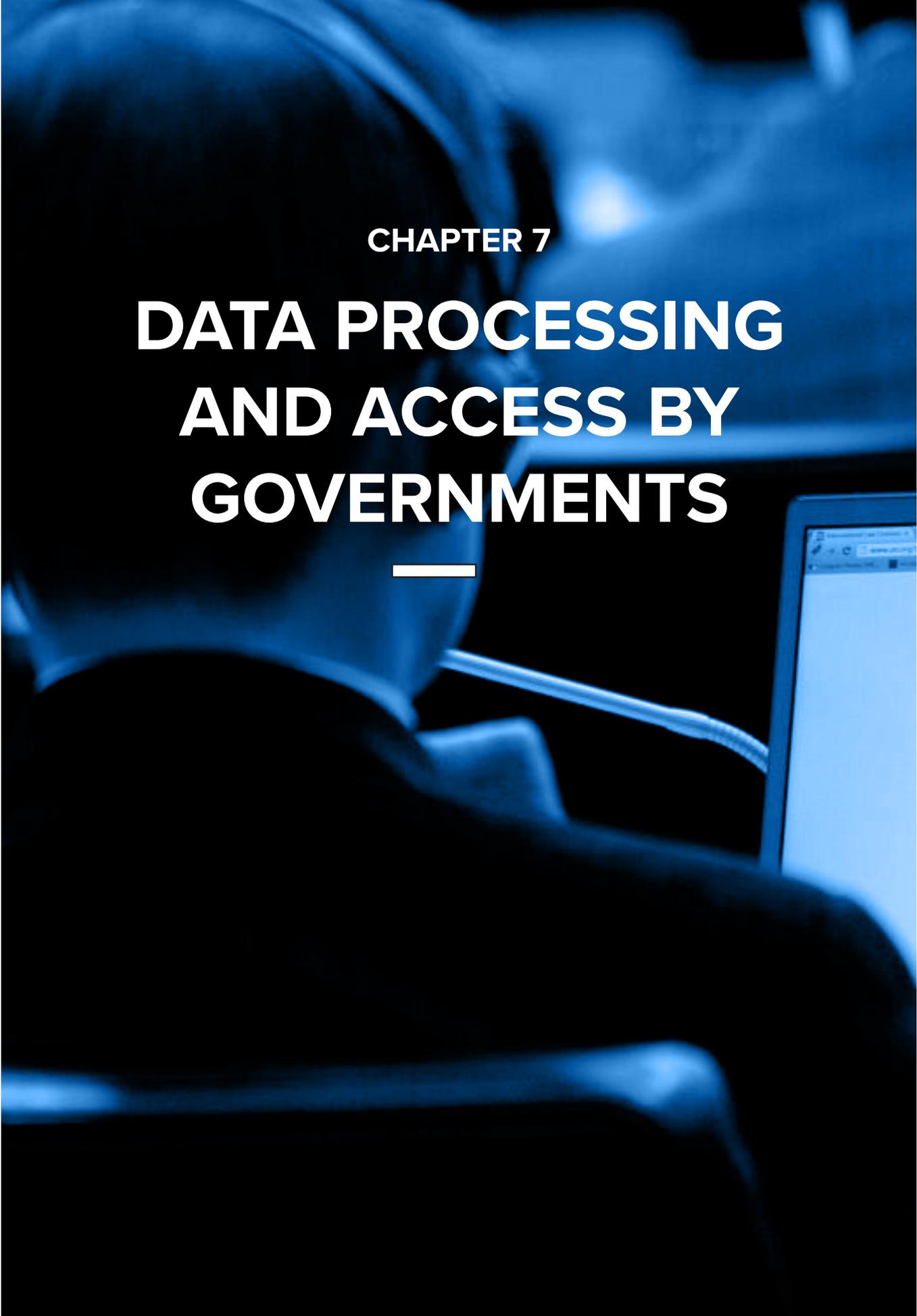
Additionally, government agendas should include the promotion of digital literacy among children, adolescents, teachers, and parents. In 2014, the Czech Republic proposed a Digital Education Strategy aimed at ensuring: non-discriminatory access to digital educational resources; conditions for development of digital skills in students and teachers; the reinforcement of educational infrastructure, and; the encouragement of the integration and understanding of digital technologies into schools.⁵³⁹



537 APEC Privacy Framework. Section V, para 26, page 15

538 Consultative Committee on Convention 108, 'Guidelines on Children's Data Protection in an Education Setting' (2020) <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b>; Lisa Archbold and others, 'Children's Privacy In Lockdown: Intersections Between Privacy, Participation And Protection Rights In A Pandemic' (2021) 3 *Law, Technology and Humans* 28 <https://lthj.qut.edu.au/article/view/1803>.

539 Ministry of Education, Youth and Sports, 'The Digital Education Strategy Until 2020' (Prague 2014) <https://www.msmt.cz/vzdelavani/skolstvi-v-cr/strategie-digitalniho-vzdelavani-do-roku-2020?lang=1>.

A person in a dark suit is shown in profile, working at a computer. The scene is dimly lit with a strong blue color cast. The person's hands are on a keyboard, and a computer monitor is visible on the right side of the frame. The overall atmosphere is professional and focused.

CHAPTER 7

**DATA PROCESSING
AND ACCESS BY
GOVERNMENTS**

7.1 Introduction

Governments have long accessed data and carried out lawful surveillance for the purposes of detecting and preventing crime and maintaining public order. These goals have broadly been interpreted and accepted as legitimate aims on the basis of which states may access and use personal data, subject to certain safeguards.⁵⁴⁰ Methods of surveillance have continued to evolve as technologies and communication systems advance and range from physical tracking and spying, to intercepting and opening telegrams. In the digital age, far more sophisticated systems for data surveillance have been created.⁵⁴¹

Reasons for data collection and access have been expanding beyond the traditional objectives of law enforcement and national security. Governments have increasingly begun to collect citizens data on the grounds that they wish to improve and render more efficient the delivery of public services. For instance, the national digital identification programmes of Kenya, India, Estonia, and Spain were built with the goal of better assisting the targeted delivery of services.⁵⁴²

It is no longer debateable that governments have a clear and compelling need to collect and process personal data.⁵⁴³ This access, however, together with permissive legislative and regulatory frameworks for surveillance increases the scope for privacy violations of citizens. As a measure to protect the privacy of citizens, data protection laws should take into account data protection principles when regulating the collection, access, and use of personal data by governments and their agencies.

540 Jeffrey L Vagle, *Being Watched- – Legal Challenges To Government Surveillance* (New York University Press 2017); United Nations Human Rights Council, 'The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights' UN Doc A/HRC/27/37 (2014). https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

541 'The Evolution Of Spy Tools' (Forbes, 2006) https://www.forbes.com/2006/04/15/intelligence-spying-gadgets_cx_lh_06slate_0418tools.html?sh=6cc700ee65c0; *Malone v United Kingdom* (1984) 7 EHRR 14; United Nations General Assembly, 'The Right To Privacy In The Digital Age' UN Doc A/RES/68/167 (2013) <https://undocs.org/A/RES/68/167>.

542 'The Aadhaar database has been upheld as constitutional in *Puttaswamy v UOI*, AIR 2017 SC 4161 <https://privacylibrary.ccg.nlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>; See Hudma Namba FAQs 1 and 2, Huduma Namba, 'Frequently Asked Questions' <https://www.hudumanamba.go.ke/faqs/>; e-Estonia, 'e-Identity' <https://e-estonia.com/solutions/e-identity/id-card/>; 'Spain's Digital Private Individual Certificate' <https://www.sede.fnmt.gob.es/en/certificados/persona-fisica>.

543 Jason M. Weinstein, William L. Drake and Nicholas P. Silverman, 'Privacy Vs. Public Safety: Prosecuting And Defending Criminal Cases In The Post-Snowden Era' (2015) 52 *American Criminal Law Review* 729.



While there are variations in how language is used in the major human rights conventions, the corpus of international human rights law (including the jurisprudence of the UN Human Rights Committee, the ECtHR, the European Court of Justice (ECJ), the Inter-American Court of Human Rights (IACHR), and the African Court on Human and Peoples' Rights (African Court) generally recognises and reconciles the apparent tension between legitimate state interests and privacy, by requiring that governmental access to personal data meets certain standards.⁵⁴⁴ Given that such access to personal data constitutes a prima facie limitation of the right to privacy, it must conform to the requirements that can be distilled from this body of jurisprudence.

This chapter details the safeguards that are applicable to governmental access to personal data, and proceeds as follows:

- **First principles of governmental access to personal data under international human rights law (section 7.2);** Restrictions to the right to privacy and related rights must be: (i) provided for by law; (ii) not be arbitrary; (iii) pursue a legitimate aim; and (iv) be necessary and proportional to achieving such legitimate aim.
- **Exemptions that governments can legitimately claim from data protection obligations (section 7.3);** Typically, frameworks allow exemptions for: (i) national security and investigation of crimes; (ii) regulatory functions; and (iii) broader exemptions, subject to adequate data security safeguards.

544 UN Human Rights Council, 'The Right To Privacy In The Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' UN Doc A/HRC/27/37 (2014) https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

7.2 Government access to personal data and the first principles of international human rights law

Under international human rights law, restrictions on the right to privacy and related rights, including the right to freedom of expression and association, must:

- be provided for by “law”;⁵⁴⁵
- not be “arbitrary”;⁵⁴⁶
- pursue a “legitimate aim”;⁵⁴⁷ and
- the restriction must be “necessary” and “proportional” to achieving such legitimate aim.⁵⁴⁸

Lawful restrictions on the right to privacy and related rights are required to comply with all the factors described above. In the context of government access to personal data, measures allowing access must be authorised by law. Such laws must ensure that the collection, access, and use of communications data by the state are carried out only pursuant to specific legitimate objectives.

The laws must also specify the circumstances in which interferences by states are allowed, besides authorisation procedures, limits on data retention and storage, as well as oversight procedures over such state access.⁵⁴⁹

7.2.1 Restrictions on the right to privacy and related rights must be provided for by law

Any measure allowing government agencies access to personal data must have a legal basis or be provided for in a law. This includes laws in their formal sense, such as national legislation, regulations, rules, ordinances, and judicial decisions, as well as other state instruments that are of a binding nature, such as government schemes, policies, etc.⁵⁵⁰ Data protection legislation often excludes data access for regulatory purposes, law enforcement, or national security purposes from adherence with its provisions.

545 Para 3 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (1988) para 3 <https://www.refworld.org/docid/453883f922.html>; UN Human Rights Council, “The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights” UN Doc A/HRC/27/37 (2014) https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

546 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (1988) para 4 <https://www.refworld.org/docid/453883f922.html>; UN Human Rights Council, “The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights” UN Doc A/HRC/27/37 (2014) https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

547 6. UN Human Rights Committee (HRC), General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant (2004) CCPR/C/21/Rev.1/Add.13, para 36 <<https://www.refworld.org/docid/478b26ae2.html>>; UN Human Rights Council, “The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights” UN Doc A/HRC/27/37 (2014) https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf accessed 13 December 2021.

548 UN Human Rights Committee (HRC), General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant (2004) CCPR/C/21/Rev.1/Add.13, para 6 <https://www.refworld.org/docid/478b26ae2.html>; UN Human Rights Council, “The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights” UN Doc A/HRC/27/37 (2014) https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

549 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (1988) <https://www.refworld.org/docid/453883f922.html>; UN Human Rights Council, “The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights” UN Doc A/HRC/27/37 (2014). https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

550 Manfred Nowak, U.N. Covenant On Civil And Political Rights: CCPR Commentary (1993) 382.

“The requirement to be provided for ‘by law’ also implies that such laws should be accessible and sufficiently precise to lay persons to allow them to regulate their conduct accordingly, and predictable enough to enable them to foresee the consequences of their conduct.”

Government access may be authorised under separate laws that may provide for adequate safeguards against possible abuse.⁵⁵¹ The mere enactment of a law authorising surveillance, however, would not satisfy the requirement of legality. The requirement to be provided for ‘by law’ also implies that such laws should be accessible and sufficiently precise to lay persons to allow them to regulate their conduct accordingly, and predictable enough to enable them to foresee the consequences of their conduct.⁵⁵²

For instance, when dealing with the handling of personal information by the Romanian intelligence services in *Rotaru v Romania*, the ECtHR ruled that the national law did not clearly define the type of information that could be processed, the categories of individuals who could be surveilled, the circumstances under which the surveillance would occur, or the procedure to be followed.⁵⁵³ Importantly, while secret rules or legislation do not satisfy this requirement of clarity or predictability, the ECtHR has also noted that in the context of covert surveillance, it is enough if the national law contains adequate indications as to the circumstances and conditions for surveillance.⁵⁵⁴

With specific regard to secret rules, the creation of a ‘surveillance database’ was found in *Shimovolos v Russia* to be in violation of ECHR’s right to privacy because it was governed by a ministerial order that was not published or made available to the public. Additionally, the ECtHR ruled that the ministerial order did not have sufficient clarity regarding the domestic authorities’ powers to collect and store personal information in the database, and that the interference was therefore not “in accordance with the law.”⁵⁵⁵

551 I. S. Rubinstein, G. T. Nojeim and R. D. Lee, 'Systematic Government Access To Personal Data: A Comparative Analysis' (2014) 4 International Data Privacy Law.

552 UN Human Rights Committee, General Comment no. 34: Article 19, Freedoms of opinion and expression (12 September 2011) <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

553 *Rotaru v. Romania*, (2000) ECHR 192 <https://privacylibrary.ccg.nlud.org/case/rotaru-vs-romania>.

554 *Silver and others v. the United Kingdom*, (1983) 5 EHRR 347, paras. 85-86; *Malone v United Kingdom* (1984) 7 EHRR 14 para. 67.

555 *Shimovolos v. Russia*, (2011) ECHR 987.

7.2.1.1 Framework overview of the requirement for restrictions on the right to privacy and related rights to be provided for by law

The exemption from data protection obligations under the frameworks are typically required to be based on clear and accessible laws. Convention 108+, the APEC Privacy Framework, the OECD Guidelines and the OAS Principles all acknowledge that exemptions from data protection obligations should be authorised by law and accessible to the public.⁵⁵⁶ The OAS Principles also require such laws to include the right of data subjects to be informed about any restrictions to the application of the principles, unless it would be incompatible with the purposes of such restrictions. They also note some of the details that any laws restricting the application of the principles should have, including the categories of data, scope of restrictions, and possible risks to the rights and freedom of data subjects, among others.⁵⁵⁷

7.2.2 Restrictions on the right to privacy and related rights must not be arbitrary

Even if government access is provided for under law, restrictions on the right to privacy and related rights would contravene the principles of international human rights law if they are arbitrary. According to the UN Human Rights Committee, the requirement against “arbitrary interference” is meant to guarantee that even interference provided for by law should be in accordance with the aims and objectives sought to be achieved by such interference, and be reasonable.⁵⁵⁸ The requirement of non-arbitrariness and legality also means that the law should sufficiently lay down procedures for oversight and accountability.⁵⁵⁹ For instance, in *Benedik v. Slovenia*, the ECtHR found that a law used by the police to collect subscriber information that did not have any independent supervision mechanisms did not offer sufficient safeguards against abuse. It also concluded that interference with the right to respect private life was not in accordance with the law, as required by Article 8 of the ECHR.⁵⁶⁰



556 Convention 108+, art. 11(1); APEC Privacy Framework, Part I, para 18; OECD Guidelines, Chapter 1, Part 1, para 4; and OAS Principles with Annotations, Principle 12, p 27.

557 OAS Principles with Annotations, Principle 12, p 27.

558 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, (8 April 1988) para 4 <https://www.refworld.org/docid/453883f922.html>.

559 In *Benedik v Slovenia*, the ECtHR found that the law used by the police to obtain metadata on a subscriber without his consent, did not have any independent supervision of the use of these police powers, *Benedik v. Slovenia*, Application No 62357/14, 130.

560 *Benedik v. Slovenia*, Application No 62357/14, 130.

Box 7.1: The ECtHR's Minimum Standards for Surveillance Legislation⁵⁶¹

- The offences and activities in relation to which surveillance may be ordered must be spelled out in a clear and precise manner.
- The law must clearly indicate which categories of people may be subjected to surveillance.
- There must be strict time limits on surveillance operations.
- Strict procedures must be in place for ordering the examination, use, and storage of the data obtained through surveillance.
- The law must lay down the precautions to be taken when communicating collected data to third parties.
- There must be strict rules on the destruction or erasure of surveillance data to prevent surveillance from remaining hidden after the fact.
- The bodies responsible for supervising the use of surveillance powers must be independent and responsible to, and be appointed by, the legislature rather than the executive.

561 *Klass and Others v. Germany, Liberty and Others v. the United Kingdom*, Application No 58243/00, 1 July 2008 and *Rotaru v. Romania*, no. 28341/95,[GC], 4 May 2000 concerning surveillance carried out by the intelligence agencies <https://privacylibrary.ccg.nlud.org/case/rotaru-vs-romania>; Electronic Frontier Foundation and Article 19, 'Necessary & Proportionate, International Principles On The Application Of Human Rights Law To Communications Surveillance Background And Supporting International Legal Analysis' (2014) p 17 <https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf>.

7.2.3 Legitimate aims for restrictions on the right to privacy and other rights: national security and the prevention and investigation of crimes

International human rights instruments, including the ICCPR and the ECHR, also provide that restrictions on human rights, such as government access to personal data, must pursue a legitimate aim. The legitimate aims in these instruments are typically broadly phrased, such as national security, public safety, as well as the prevention and investigation of crime.⁵⁶² These are also found in data protection frameworks, and they exempt states and their agencies from compliance with data protection obligations. As will be shown in subsequent sections, the body of jurisprudence from these instruments can be helpful in interpreting the corresponding exemptions in data protection frameworks. For instance, the Explanatory Report to Article 11 of Convention 108+ states that the notion of 'national security' should be "interpreted on the basis of the relevant case law of the European Court of Human Rights."⁵⁶³

7.2.3.1 National security

With an increase in major ongoing international terrorist threats, the focus of security policies, throughout much of the world, has shifted from an ex post facto approach (punishment after the act) to a preventative one that seeks to avoid the incidence of security-related crimes. This forms the background and context to revelations of a few years ago when extensive surveillance programmes by intelligence agencies the world over were justified on the grounds of national security.⁵⁶⁴

Although all Identified Regional Frameworks (except the AU Convention) include 'national security' as grounds for exemption from data protection obligations, none of them define the term. The AU Convention uses the term 'state security', but also does not define it.⁵⁶⁵ Furthermore, the APEC Privacy Framework, the ASEAN DP Framework, the OAS Principles and the OECD Guidelines also recognise national sovereignty as grounds for exemption.⁵⁶⁶ Justifications such as public safety, public security and public policy are also found in the frameworks.⁵⁶⁷

Despite attempts being made in various contexts, there is no universally accepted definition of 'national security' or the related grounds described above, either within UN jurisprudence or among other international organisations. According to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (Johannesburg Principles), restrictive measures that purportedly aim to protect national security have to "protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government."⁵⁶⁸ Measures that only seek to protect a government from exposure of wrongdoing, or conceal information about the functioning of its public institutions, or entrench a particular ideology, or suppress industrial unrest, are specifically disavowed as being unrelated to national security.

562 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 (ECHR), art. 8(2). https://www.echr.coe.int/documents/convention_eng.pdf.

563 Explanatory Report to Convention 108+, Para 92, p 26.

564 Arianna Vidaschi, 'Privacy And Data Protection Versus National Security In Transnational Flights: The EU-Canada PNR Agreement' (2018) 8 International Data Privacy Law 124-139; UN Human Rights Council, "The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights" UN Doc A/HRC/27/37 (2014). https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

565 Art. 9(1)(d), AU Convention, art 19 (1) (d)

566 APEC Privacy Framework, para 18; ASEAN DP Framework, para 4(b); OAS Principles with Annotations, Principle 12; OECD Guidelines, Chapter 1, Part 1, para 4.

567 APEC Privacy Framework, Part I, para 18; ASEAN DP Framework, para 4; AU Convention, Art. 9 (1) (d); HIPCAR Model Legislative Text, s 35; OECD Guidelines, Chapter 1, Part 1, para 4.

568 The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1996), Principle 2(a), art 19

Similarly, the Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR (Siracusa Principles) that elaborate the grounds for ICCPR limitations, provide that national security can be invoked to justify measures restricting human rights “only when they are taken to protect the existence of the nation or its territorial integrity or political independence.” The Siracusa Principles also stipulate that national security cannot be invoked to impose limitations in cases of isolated incidents of law and order.⁵⁶⁹

Reference to international human rights case law shows that contestations between national security and impacted rights, such as the right to privacy, are dealt with on a case-by-case basis.⁵⁷⁰ Indeed, some case law suggests that an exhaustive definition may not be possible. In *Esbester v The United Kingdom*, the European Commission on Human Rights (now decommissioned) dismissed the complaint by the plaintiff who argued that his privacy had been violated because secret files on his life had been maintained by special police forces, and that the term ‘national security’ had too wide an ambit. The Commission ruled that the plaintiff’s rights were not violated in this case, and that as long as there were sufficient safeguards along with the measures restricting the rights of the individual, a “comprehensive definition of the notion.....of national security” was not required.⁵⁷¹

In line with this view, the ECtHR’s case law has focused on the conditions with which measures pertaining to national security must comply in order for interferences with the right to privacy and data protection be justified. In the context of the ECHR’s Article 8 right to respect for one’s private life, these

conditions stipulate that interference should be in accordance with the law and justified by legitimate aims, and that they must be necessary in a democratic society.⁵⁷²

Common threads can be identified from case law, however, to gain a better sense of how the legitimate aim of national security is usually applied in the context of the right to privacy and government access to personal data. For instance, storing personal data in a secret police register for the purpose of vetting appointees to sensitive posts in public service was accepted by the ECtHR as appropriately justified by the need for ‘national security.’⁵⁷³ Similarly, surveillance of a person in connection with terrorist activity was also viewed as suitably serving the interests of national security.⁵⁷⁴

7.2.3.2 Law enforcement purposes

Collection of data for law enforcement purposes also constitutes an interference with the right to privacy, and hence must be based on a clear, accessible law that pursues a legitimate aim, and is limited to measures that are necessary and proportionate to achieve that purpose.⁵⁷⁵ Law enforcement purposes vis-à-vis access to personal data commonly include the “prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against the prevention of threats to public security.”⁵⁷⁶ Personal data may usually be accessed by law enforcement agencies for any of these purposes. Relevant agencies for law enforcement include police, criminal courts, and other public or statutory bodies whose functions are relevant for the purposes

569 The Siracusa Principles on Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, American Association for the International Commission of Jurists (1985), paras 29-30

570 *Malone v United Kingdom* (1984) 7 EHRR 14; *Toonen v Australia*, Communication No. 488/1992, (1994) UN Doc CCPR/C/50/D/488/1992; *Peck v United Kingdom* (2003) 36 EHRR 41; *Antonius Cornelis Van Hulst v Netherlands* Communication No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999 (2004); *S and Marper v United Kingdom* (2008) ECHR 1581 <https://privacylibrary.ccgnlud.org/case/s-and-marper-vs-united-kingdom?searchuniqueid=566305>; *Tristán Donoso v Panamá* (2009) IHRL 3064 (IACHR 2009); *Escher v Brazil* IACHR (ser. C) No. 200/2009; *Fontevecchia and D’amico v. Argentina* Am. Ct. H.R. (ser. C) No. 238/2011 <https://privacylibrary.ccgnlud.org/case/fontevecchia-and-damico-vs-argentina?searchuniqueid=345563>; *G v Australia* (2017), CCPR/C/119/D/2171/2012.

571 *Esbester v. The United Kingdom*, European Commission of Human Rights, Application No. 18601/91.

572 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, art. 8

573 *Leander v. Sweden*, IHRL 69 (ECHR 1987), 49.

574 *Uzun v. Germany*, Application No. 35623/05, (ECHR 2010),77.

575 Council of Europe, ‘Practical Guide On The Use Of Personal Data In The Police Sector’ T-PD(2018)01 (Directorate General of Human Rights and Rule of Law 2018) 3 <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

576 UK Data Protection Act 2018 (c. 12),s 31.

of law enforcement specified above and include revenue authorities among others.

Case law in Europe provides additional detail on the meaning of the broadly worded ‘law enforcement’ justification as a legitimate aim to restrict the right to privacy and other rights. In *Uzun v Germany*, the ECtHR ruled that surveillance of the applicant via GPS did not violate the applicant’s right to respect for private life because the applicant was being investigated in connection with terrorist bombings. The surveillance was therefore pursuant to the legitimate aims of preventing crime and protecting national security and public safety.⁵⁷⁷ *Ben Faiza v France* is another example of what could constitute a justification for law enforcement purposes. In this case, the applicant’s call records had been obtained to triangulate his location pursuant to an investigation concerning the import of drugs, criminal conspiracy, and money laundering. The ECtHR ruled that the measure was justified since it was aimed at pursuing a drug-trafficking operation.⁵⁷⁸

Just as data controllers and processors are accountable when collecting and processing personal data, so are law enforcement agencies. The CoE’s Practical Guide on Use of Personal Data in the Police Sector recommends that personal data collected at the early stages of the investigation should not continue to be processed if it is found no longer relevant. Police should also regularly ask themselves if collecting data is necessary for a particular investigation or task. An individual’s data should only be processed when there is a link between the person whose data is processed and the purpose of processing (for example, for the investigation or offence). This link should always be demonstrable.⁵⁷⁹

“Collection of data for law enforcement purposes also constitutes an interference with the right to privacy, and hence must be based on a clear, accessible law that pursues a legitimate aim, and is limited to measures that are necessary and proportionate to achieve that purpose”

577 *Uzun v. Germany*, Application No. 35623/05, (ECHR 2010)

578 *Ben Faiza v. France*, Application no. 31446/12, (ECHR 2018), para 59.

579 Council of Europe, ‘Practical Guide On The Use Of Personal Data In The Police Sector’ T-PD(2018)01 (Directorate General of Human Rights and Rule of Law 2018) 3 <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

Box 7.2: Germany's High Threshold for Legitimate Aim(s)

In 2008, the German Federal Constitutional Court invalidated several provisions of the North-Rhine Westphalian Act on the Protection of the Constitution which authorised the government to conduct online surveillance of IT infrastructure such as personal computers. The Court ruled that to qualify as legitimate grounds for surveillance, there would have to be factual evidence of “a concrete threat to an important legally-protected interest,” such as a threat to the “life, limb or liberty of a person” or to “public goods, the endangering of which threatens the very bases or existence of the state, or the fundamental prerequisites of human existence.”⁵⁸⁰

7.2.4 Restrictions on the right to privacy and related rights must be necessary and proportionate to the legitimate aim pursued

National authorities and policymakers have a range of measures and instruments to achieve a given objective. When choosing which measure or instrument to employ, any negative impact on rights, including the right to privacy, has to be considered. This is why restrictions or interference with the right to privacy have to be necessary, as well as proportional to the legitimate aim pursued. According to the UN

Human Rights Committee, the ‘necessity’ requirement is met when, in addition to serving legitimate aims, the interference is essential to achieving those aims.⁵⁸¹ It states that the interference must not just serve the legitimate aims, but also be necessary to protect them. The restrictive measures must conform to the principle of proportionality, and must be:

- “appropriate” to protect the legitimate aims;
- the “least intrusive instrument which might achieve the desired result”; and
- “proportionate to the interest” sought to be protected.⁵⁸²

580 BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -,1-333, http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

581 UN Human Rights Committee (HRC), CCPR General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9, 223 – 227, 11 – 16 <https://www.refworld.org/pdfid/45139c394.pdf>.

582 UN Human Rights Committee (HRC), CCPR General Comment No. 27: Article 12 (Freedom of Movement), (1999) CCPR/C/21/Rev.1/Add.9, 223–227, 11 – 16 <https://www.refworld.org/pdfid/45139c394.pdf>. Although these comments are made in the context of the freedom of movement, they are applicable to the right to privacy under Art. 17 of the ICCPR. See UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/13/37, (28 December 2009), para. 11 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf.

Notably, the principle of necessity is interspersed throughout data protection law. For instance, data minimisation, an important principle of data protection, is based on the understanding that only the necessary amount of data, and not more information, should be collected to achieve a given legitimate objective. The necessity and proportionality tests that currently apply to personal data protection originally evolved in the context of the right to privacy.⁵⁸³ The ECtHR's case law is helpful in understanding this evolution. In *Klass v Germany*, the ECtHR accepted that legislation authorising surveillance was necessary in a democratic society' in the interests of national security and/or preventing crime. At the same time, it ruled that the provisions of such legislation and surveillance measures had to be strictly necessary to safeguard democratic institutions.⁵⁸⁴

Subsequently, in *Weber and Saravia v Germany*, the ECtHR reiterated that surveillance measures could be necessary for the protection of national security, and that national authorities enjoyed a margin of appreciation in choosing which measures to employ that best suited the objectives.⁵⁸⁵ However, the Court ruled that such measures could only exist with sufficient and adequate guarantees against abuse, the assessment of which depended on factors such as the "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."⁵⁸⁶

In *Kennedy v United Kingdom*, while examining the proportionality of the UK's Regulation of Investigatory Powers Act which authorised surveillance, the ECtHR noted that:

- citizens had adequate indication as to the circumstances in which they could undergo

surveillance;

- surveillance itself was conditional of a warrant;
- the warrant had to sufficiently specify categories of persons and the personal data that could undergo surveillance, and;
- the warrant had an expiry date after which it would have to be renewed.⁵⁸⁷

The ECtHR also noted that obtaining and renewing the warrant was conditional on showing that it was necessary and that there were sufficient oversight procedures to prevent abuse.⁵⁸⁸

This test for necessity and proportionality has been adopted in varying forms by several jurisdictions across the world. In 2017, the Indian Supreme Court, while clarifying that the Indian Constitution guaranteed a right to privacy to Indian citizens, ruled that measures interfering with this constitutional right would have to pass the proportionality test. The Court, via a plurality opinion, ruled that there has to be a "rational nexus between the objects...and the means to achieve them."⁵⁸⁹ Although the understanding and application of this test continues to evolve within India's national context, the proportionality test has now become a standard feature of privacy and data protection law.⁵⁹⁰

The European Data Protection Supervisor (EDPS), an independent authority meant to ensure and monitor the consistent enforcement of data protection rules within EU institutions, bodies, and agencies, has issued guidance explaining the substance of necessity and proportionality tests. As per the toolkit issued by the EDPS, the general approach is to ascertain whether a measure is actually necessary before proceeding to whether it is proportional. It should be noted that the toolkit also recognises a certain overlap between necessity and proportionality.⁵⁹¹

583 Opinion of the Art. 29 Working Party, 27.02.2014, p. 3-4. The Art. 29 Working Party has noted that the right to privacy under Art. 8 of the European Convention of Human Rights has a clear link with the right to personal data protection under Art. 7 of the European Charter of Fundamental Rights.

584 *Klass v Federal Republic of Germany*, IHRL 19 (ECHR 1978), 42, 48.

585 *Weber and Saravia v. Germany*, Application no. 54934/00, (ECHR 2006), 106.

586 *Weber and Saravia v. Germany*, Application no. 54934/00, (ECHR 2006), 106.

587 *Kennedy v United Kingdom* [2010] ECHR 682 (18 May 2010), 159 – 169.

588 *Kennedy v United Kingdom* [2010] ECHR 682 (18 May 2010), 159 – 169.

589 *Justice KS Puttaswamy v UOI*, AIR 2017 SC 4161, J. Chandrachud <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>.

590 *Justice KS Puttaswamy v UOI*, AIR 2017 SC 4161 <<https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>>; *Justice KS Puttaswamy v Union of India* (2019) 1 SCC 1 <<https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uoi-and-ors>>; India, The Draft Personal Data Protection Bill, 2019 currently being reviewed by a parliamentary committee available at <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 13 December 2021..

591 European Data Protection Supervisor, 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (EDPS 2017) 5-6 https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

Box 7.3: The EDPS Checklist for ‘Necessity’ and ‘Proportionality’ Assessment of Legislative Measures⁵⁹²

The Office of the EDPS has formulated a helpful checklist to determine whether a proposed legislative measure satisfies the necessity and proportionality requirements.

When assessing necessity, the following steps may be followed:

Step 1 – Is there a factual description of the measure and its purpose?

Step 2 – Does the proposed measure/data processing limit any particular right under data protection law or otherwise?

Step 3 – Are the objectives of the measure defined?

Step 4 – Is the proposed measure effective and the least intrusive?

To assess proportionality, the following steps may be followed -

Step 1 – Advantages: Is the objective legitimate? Does the proposed measure achieve the objective and if yes, to what extent?

Step 2 – Disadvantages: What is the scope, the extent and the gravity of limitation on the rights under data protection law? Furthermore, what is the scope, the extent and the gravity of limitation on the rights to privacy?

Step 3 – Do the advantages outweigh the disadvantages?

Step 4 – If the disadvantages outweigh the advantages, what safeguards could make the advantages outweigh the disadvantages?

Jurisdictions such as Jamaica have also adopted tests of necessity and proportionality when assessing the constitutional validity of national identity databases that collect personal data, including biometric data. In its ruling on challenges to the implementation of the National Integrated Identity Management System (NIIMS) or the *Huduma Namba* digital database, the High Court of Kenya recalled Canadian jurisprudence and ruled that assessing proportionality was a two-step test.

The first step called for the law to be enacted with a proper purpose whereas the second step includes three components, which require that: (i) the measure must be carefully designed to achieve the objective; (ii) the means must violate the right as little as possible; and (iii) there must be proportionality between the measure and the effect, i.e., the benefit must be greater than the harm to the right. In the end, Kenya’s High Court ruled that the country’s NIIMS, as at that time designed, did not satisfy the proportionality test.⁵⁹³

592 European Data Protection Supervisor, ‘Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit’ (EDPS 2017) 5-6 https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

593 Nubian Human Rights Forum and Ors. v The Hon. Attorney General and Ors., Petition 56, 58, and 59 of 2019 (Consolidated), (2020) eKLR, 915, 922 <https://privacylibrary.ccgmlud.org/case/nubian-rights-forum-2-ors-vs-attorney-general-6-ors?searchuniqueid=130591>.

7.2.4.1 Framework overview of necessity and proportionality requirements

Several of the Identified Regional Frameworks have incorporated these principles. According to Convention 108+, exceptions to compliance with data protection obligations and protection of the rights of data subjects include those on the grounds of national security and prevention and investigation of crimes, but should be provided by law only to the extent that they constitute “necessary and proportionate measure(s) in a democratic society” to fulfil such aims.⁵⁹⁴ Although Convention 108+ additionally uses the term ‘proportionate’, the language is notably reminiscent of the language used in the exception to the right to privacy of the ECHR’s Article 8.⁵⁹⁵

The Commonwealth Privacy Bill also incorporates the necessity principle when allowing compliance exemptions for data protection obligations for the purposes of preventing and detecting crime, or which are in the interests of national security.⁵⁹⁶ The GDPR specifically requires restrictions on these grounds to be “necessary and proportionate measures in a democratic society.”⁵⁹⁷ Similarly, the HIPCAR Privacy Framework acknowledges that measures based on these exemptions should be ‘necessary.’⁵⁹⁸

The OAS Principles provide that derogations or exceptions to data protection principles should “only be implemented after the most careful consideration of the importance of protecting individual privacy, dignity and honour.” National authorities should balance “the need for the data in limited circumstances and due respect for the privacy interests of individuals.”⁵⁹⁹ Despite the fact that neither necessity

nor proportionality are specifically mentioned, their essence is incorporated to some extent.

The APEC Privacy Framework acknowledges that restrictive measures should account for their impact on rights,⁶⁰⁰ but does not otherwise refer to necessity nor proportionality. The OECD Guidelines also only state that “exceptions to the Guidelines on the grounds of national sovereignty, national security, public safety and public policy should be as few as possible”⁶⁰¹ without any reference to the twin principles of necessity and proportionality. The ASEAN DP Framework and AU Convention appear to grant broad powers to national authorities to access data without explicitly limiting them by applying the principles of necessity and proportionality.⁶⁰²

7.2.4.2 Proportionality under other national and international instruments

The principle of proportionality is also recognised in some African State constitutions under their Bill of Rights’ limitation clauses. This is particularly true for those states that have developed their legal systems based on common law principles. The proportionality principle is applied to assess the constitutionality of certain acts, conduct or measures that limit the fundamental rights of individuals, including the right to privacy that is recognised as a constitutional right in several African jurisdictions.⁶⁰³ The African Court, however, is yet to pronounce judgments relating to the proportionality principle in the context of privacy.

594 Convention 108+, art 11(3)

595 Whereas Art. 8(1) of the ECHR guarantees the right to respect for privacy and family life, Art. 8(2) allows for interferences where they are “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

596 Commonwealth Privacy Bill, s 10 (c)(f)

597 GDPR, art 13 and recital 19.

598 Explanatory Notes to the HIPCAR Model Legislative Text, s 35, para 52.

599 OAS Principles with Annotations, Principle 12, p 26,

600 APEC Privacy Framework, Part I, para 18 (Nonetheless, Economies should take into consideration the impact of these activities upon the rights, responsibilities and legitimate interests of individuals and organizations.)

601 OECD Guidelines ‘ para 4

602 ASEAN Data Protection Framework para 4(b); AU Convention, art. 9(1)(d).

603 These include Zimbabwe, South Africa, Namibia, Botswana, Zambia, Nigeria, Liberia, Cote d’Ivoire, Kenya, Guinea, Gambia, Senegal, Togo, Niger, Benin, Guinea-Bissau, Ghana, Tanzania, Uganda, Ethiopia, Rwanda, Somalia, Lesotho, and Burundi. See Media Defence, ‘Scope and the Right to Privacy’, Module 4: Privacy and Security Online, available at <https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/scope-and-the-right-to-privacy/#footnote--3>; see also George Barrie, ‘The Application Of The Doctrine Of Proportionality In South African Courts’ [2013] 28 African Journal of Public Law 40 <https://journals.co.za/doi/abs/10.10520/EJC153152>.



Based on the UNHRC, ECHR and ECJ jurisprudence, as well as the body of modern data protection laws, it is evident that the test of necessity and proportionality has become a cornerstone of data protection.⁶⁰⁴ At the international and regional levels, the UNHRC,⁶⁰⁵ acting as the interpretative body on the ICCPR and the ECHR, has consistently ruled that privacy-intrusive measures by governments should be necessary and proportional.⁶⁰⁶ The IACHR has also ruled in a series of decisions that restrictions on privacy must comply with principles of legality, necessity and proportionality.⁶⁰⁷ Although not with respect to privacy, the African Court has also held that interferences with human rights have to be such as provided by law and are necessary.⁶⁰⁸

While formulations of the test may vary, the fundamental requirements of specificity, being rationally connected to the purpose and only imposing the least intrusive measure remain the same across jurisdictions.

- 604 Ilian Mitrou and Maria Karyda, "EU'S Data Protection Reform And The Right To Be Forgotten - A Legal Response To A Technological Challenge?" [2012] 5th International Conference of Information Law and Ethics 3 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245.
- 605 Toonen v Australia (1994) CCPR/C/WG/44/D/488/1992; Antonius Cornelis Van Hulst v Netherlands (2004) CCPR/C/82/D/903/1999; G v Australia (2017), CCPR/C/119/D/2171/2012.
- 606 S and Marper v United Kingdom (2008) Application nos. 30562/04 and 30566/04 <https://privacylibrary.ccg.nlud.org/case/s-and-marper-vs-united-kingdom?searchuniqueid=652088>; Peck v United Kingdom (2003) 36 EHRR 4; Malone v United Kingdom (1984) ECHR 10.
- 607 Fontevecchia and D'amico v. Argentina Am. Ct. H.R. (ser. C) No. 238/2011 <https://privacylibrary.ccg.nlud.org/case/fontevecchia-and-damico-vs-argentina?searchuniqueid=345563>; Tristán Donoso v Panamá IHRL 3064 (IACHR 2009); Escher v Brazil IACHR (ser. C) No. 200/2009.
- 608 Tanganyika Law Society and the Legal and Human Rights Centre v. Tanzania, Application No. 011/2011; Rev. Christopher R. Mtikila v. Tanzania Application No. 009/2011.

Box 7.4: Bulk Data Collection and Retention is Permissible Only with Suitable Safeguards

In *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*, the European Data Retention Directive was held invalid by the ECJ. The directive required all internet service providers (ISPs) and telecommunications service providers operating in Europe to collect and retain a subscriber's incoming and outgoing phone numbers, IP addresses, location data, and other key telecom and internet traffic data for a period of six months to two years.

According to the ECJ, the “retention of data for the purpose of possible access to them by the competent national authorities directly and specifically affects private life.” Since such collection and retention would constitute the processing of personal data, they would have to satisfy data protection requirements. Although the objective of the Directive to fight serious crime was legitimate, the ECJ ruled that it was still not proportional because among other reasons:

- It required the collection of data of all persons regardless of whether their conduct had a link with a serious crime;
- There was no requirement for the data itself to be relevant to any serious crime, i.e. the data collected did not have to be specific to a particular time or geographical location;
- The Directive did not lay down any objective criterion to determine access to the collected data by national authorities. There were no substantive or procedural conditions for such access. For instance, it did not state that access must be strictly restricted to prevention and detection of precisely defined serious offences;
- Access by national authorities was not made dependent on a prior review by a court or independent administrative body;
- The data was retained for a period between 6 and 24 months, but there was no distinction made between the categories of data to be retained on the basis of their usefulness for the objectives being pursued.
- The Directive also did not require the mandatory destruction of the data at the end of the data retention period.

The ECJ ruled that the Directive was invalid since it did not contain sufficient safeguards and was not in accordance with the principle of proportionality.

In 2018, the ECtHR considered the question of bulk interception and whether mass surveillance and intelligence sharing violate international law. The question in *Big Brother Watch and Others v The United Kingdom*⁶⁰⁹ revolved around, inter alia, the bulk interception of communications by the Government Communications Headquarters (“GCHQ”), being one of the United Kingdom intelligence services under the TEMPORA programme. The programme intercepted data from nearly all fibre-optic cables carrying communications in and out of the UK. Finding the bulk interception unlawful and incompatible with the conditions necessary for a democratic society, the ECtHR emphasised the distinctions between targeted and bulk interception. It set down six minimum safeguards to be set out in laws enabling interception to avoid abuses of power. These were:⁶¹⁰

- the nature of offences which may give rise to an interception order;
- a definition of the categories of people who could have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for examining, using and storing the data obtained;
- the precautions to be taken when communicating the data to other parties;
- the circumstances in which intercepted data may or must be erased or destroyed.

The Court acknowledged that some of the safeguards described above are not readily applicable to mass surveillance regimes, but nevertheless noted the need for robust substantive protection to be developed for such regimes as well, informed by safeguards developed for targeted interception measures. The Court found that bulk interception, as a preventive rather than reactive measure, is unable to meet the conditions of “necessity” and “foreseeability.” It stated “...when a State is operating such a [bulk interception] regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual’s communications might be intercepted.” In the absence of these conditions, the ECtHR held that any bulk interception law would fall foul of Article 8 of the ECHR, which protects an individual’s right to respect for their private and family life. However, the Court also noted that mass surveillance and intelligence sharing in the context of collaboration with the NSA’s PRISM and Upstream programs were not *prima facie* violative of international law.

609 *Big Brother Watch and Others v. The United Kingdom*, (2015) Applications nos. 58170/13, 62322/14 and 24960/15) <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%7D>.

610 *Big Brother Watch and Others v. The United Kingdom*, (2015) Applications nos. 58170/13, 62322/14 and 24960/15), 335.

Box 7.5: Data transfers from the European Union to the United States

In *Schrems I*, the ECJ adjudicated on the transfer and storage of the personal data of European citizens in the US. The Court invalidated the European Commission's earlier decision that upheld the adequacy of the US 'Safe Harbour' system. This system which allowed the transfer of data of EU citizens to US firms that complied with safe harbour principles. The Court found that the Safe Harbour framework did not offer equivalent protection to that in the EU. It also found that interference with fundamental rights under the Safe Harbour framework was not limited to what was strictly necessary for the purposes sought to be achieved. This was since it authorised the storage of all the personal data of all the persons whose data were transferred from the EU to the US without any differentiation, limitation or exception in the objectives pursued. That there was no objective criterion laid down for determining the limits of the access of public authorities to the data and of their subsequent use was also a contributing factor to the Court's finding.⁶¹¹

Subsequently, the ECJ's 2020 *Schrems II*⁶¹² decision examined data transfers out of the EU in greater detail. It examined the EU-US Privacy Shield, which was a legal instrument regulating the exchange of personal data between the EU and the US for commercial purposes. More than 5000 companies relied on the EU-US Privacy Shield to conduct trans-Atlantic trade. The Court found that the Shield was invalidated due to concerns of surveillance carried out by US law enforcement and government agencies. The case arose in the context of the European Commission's Standard Contractual Clauses (SCCs) permitting personal data transfers to the US among other jurisdictions. Max Schrems, the petitioner, argued that Facebook's transfers of personal data to its US headquarters could be accessed by US intelligence agencies, which, in the absence of adequate safeguards, would contravene both the GDPR and EU laws. The Court found that US law did not permit data subjects to exercise their rights before US courts and authorities. This lack of safeguards was critical to the ECJ's decision. *Schrems II* requires companies themselves to verify that reciprocal safeguards exist in countries to which personal data of European citizens are transferred. Despite the onerous increase in their responsibilities, the Court held that the mere presence of SCCs was insufficient to ensure protection to personal data whether they are in transit or transferred to a non-EU State.

611 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, (2015) Case C-311/18 ['Schrems I'].

612 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, (2020) Case C-311/18 ['Schrems II'].



7.3 Exemptions governments can legitimately claim from data protection obligations

Exemptions granted to governments from adhering to data protection regulations are typically correlated to the “legitimate aims” of an act that constitutes a *prima facie* restriction of the right to privacy or private life. It is to be noted, however, that such exemptions are tempered by the need to conform to the requirements of necessity and proportionality, laid down in a long series of cases in regional courts, particularly the several courts in the EU.

7.3.1 National security, and investigation of crimes

As discussed above, all regional data protection frameworks with the exception of the AU Convention include national security as a reason to exempt states from data protection obligations.

In addition to national security, another justification that is commonly invoked for government access across the data protection frameworks is the prevention, investigation, and prosecution of crimes. As explained in section 7.2.3 above, law enforcement agencies often seek or require access to personal data to investigate serious crimes and offences ranging from money laundering to terrorist bombings. This can take the form of accessing data which can often be sensitive, such as fingerprint and DNA profiles, vehicle registrations, CCTV surveillance, criminal records, etc.

Convention 108+, the Commonwealth Privacy Bill, HIPCAR Privacy Framework, the OAS Principles, the AU Convention and the GDPR exempt compliance with certain data protection provisions on the basis of investigation and prosecution of criminal offences.⁶¹³

⁶¹³ Convention 108+, art 11(1)(a); Commonwealth PPI Bill. s 8, 10, 11; s 35 Explanatory Notes to the HIPCAR Model Legislative Text, s 35; OAS Principles with Annotations, Principle 12, page 26; APEC Privacy Framework, para 18; AU Convention, Articles 14(2)(e) and (i); GDPR, art. 23; Recourse is within a specific directive, i.e., Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of Criminal Penalties.

This justification is, however, absent in the APEC Privacy Framework and the ASEAN DP Framework, which incorporate exemptions related to ‘public policy’ and ‘public safety.’⁶¹⁴ The OAS Principles also note that states may exempt compliance with the principles for “essential public policy prerogatives.”⁶¹⁵

7.3.2 Regulatory functions

Exemptions from complying with data protection rights and obligations for regulatory compliance are also found in some legal instruments, such as the OAS Principles, the HIPCAR Privacy Framework and the GDPR.⁶¹⁶ The HIPCAR Privacy Framework exempts data controllers from their obligations under the framework and suspends data subjects’ rights where personal data is processed pursuant to “regulatory functions required of any law.” These functions include protecting members of the public against financial loss due to dishonesty, malpractice, and similar factors, and securing the health and safety of persons at work.⁶¹⁷ The GDPR, rather broadly, provides exemptions for “monitoring, inspection or regulatory function(s) connected...to the exercise of official authority” in cases pertaining to: (i) national security, defence and public security; (ii) prevention, investigation, detection or prosecution of criminal offences; (iii) other important objectives of general public interest of the Union or a Member State, and; (iv) breaches of ethics in a regulated profession.⁶¹⁸ These grounds can be invoked to limit the scope of the rights of data subjects, as well as exempt controllers and processors from compliance with data protection principles. However, necessity and proportionality requirements still apply.⁶¹⁹

7.3.3 Data protection obligations that the state is exempt from

The exemptions provided for government agencies vary. However, most of the regional frameworks have identified specific obligations that government agencies are exempt from in cases where grounds such as national security, law enforcement and public safety are invoked.

In Convention 108+, Article 11 provides that the obligations of fair processing, purpose limitation, data minimization and data accuracy, breach notification, transparency, and data subjects’ rights, including the rights to confirmation, access, rectification, erasure and remedy do not have to be complied with for the protection of national security, defence, public safety or law enforcement.⁶²⁰ Additionally, Article 11(3) also provides further exemptions on the grounds of national security and defence. These exemptions include the preclusion of the Convention Committee from evaluating the effectiveness of the measures taken to implement the Convention, not having to provide all relevant information to the supervisory authority in case of cross-border transfers, or having to demonstrate effective safeguards in cases of cross-border transfers. The AU Convention’s prohibition on disclosure of sensitive personal data through the collection and processing of data revealing racial and ethnic origin, sex life, genetic information, etc., does not apply where a judicial procedure or criminal investigation is instituted.⁶²¹

Under the Commonwealth Privacy Bill, the national security and law enforcement justifications exempt public authorities from compliance with transparency provisions. As a result of this, the public authorities need not inform the individuals concerned of the purposes of data collection, nor the legal basis for such collection and the intended recipients of

614 ASEAN DP Framework, para 4, APEC Privacy Framework, Part I, para 18.

615 OAS Principles with Annotations, Principle 12, p 26,

616 OAS Principles with Annotations, Principle 12, p 26. It simply acknowledges that national authorities can invoke ‘regulatory compliance’ as a ground for exemption without specifying the content of the ground or the measures that could be exempted; CARICOM HIPCAR Model Legislative Texts, s 36 - Exemptions apply to compliance with obligations of data controllers and the rights of data subjects GDPR, art. 23(h).

617 HIPCAR Model Legislative Texts, s 36.

618 GDPR, art 23(h)

619 GDPR, art 23(h).

620 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, (1981) OJ 108, art 11(1)(a).

621 AU Convention, art 14 (2)(c)

the collected data.⁶²² Under the framework, public authorities are required to not share any personal information it holds with any other individual or agency. However, it is exempted from this obligation on various grounds, including for national security and law enforcement purposes.⁶²³ Although sharing of personal data across government agencies can increase efficiency and effectiveness of government services, it also increases risks to data security, due to the sharing of access to data resources and the use of personal data for uses different from the purpose for which it may have been initially collected.

In this context, the ECtHR held the measures prescribed in the United Kingdom's Regulation of Investigatory Powers Act, 2000 (RIPA) to be sufficiently robust. These measures required that personal data could be shared under the Act and should be limited to the minimum necessary for the specified purposes.⁶²⁴ The RIPA required, in this context, that the following criteria should be kept to the minimum: (i) the number of persons to whom the material or data was disclosed or made available; (ii) the extent to which the material or data was disclosed or made available; (iii) the extent to which the material or data was copied, and; (iv) the number of copies that were made.⁶²⁵ Disclosure to persons who were not vetted and did not fall under the "need-to-know" basis is prohibited.⁶²⁶

According to Article 23, the GDPR provides that on the grounds of national security, defence, and public security, EU Member States can restrict by way of a legislative measure the scope of the rights of data subjects and data controller and processor obligations. The operation of data protection principles, to the extent that they correspond to the rights and obligations provided under the GDPR can also be restricted on these grounds. These obligations are also exempt for "important objectives of general public interest," including public health.⁶²⁷

Unlike the above frameworks that limit exemptions to specific data protection obligations and rights, some regional frameworks completely exempt the application of their provisions for grounds related to national security and public safety. The APEC Privacy Framework provides that the APEC information privacy principles do not apply when government measures are invoked to protect national sovereignty, national security, public safety, and public policy.⁶²⁸ The APEC Commentary, while recognising the importance of state respect for privacy, notes that obligations under the APEC Framework are not meant to impede lawful government actions when used for these purposes.⁶²⁹

The ASEAN DP Framework allows for a broad exemption from its provisions, stating that the framework would not apply to measures adopted by states to "exempt any areas, persons or sectors from the application of the principles," as well as for matters relating to national sovereignty, national security, public safety, public policy and "all government activities deemed suitable to be exempted".⁶³⁰ The OECD Guidelines simply provide that exceptions on the grounds of national sovereignty, national security and public policy should be as few as possible and should be made known to the public.⁶³¹

622 Section 8(3)(d)(v), Model Privacy Bill, s 8(3)(d)

623 Model Privacy Bill, s 11(1).

624 *Big Brother Watch and Others v. The United Kingdom*, (2015) Applications nos. 58170/13, 62322/14 and 24960/15), 392.

625 *Big Brother Watch and Others v. The United Kingdom*, (2015) Applications nos. 58170/13, 62322/14 and 24960/15), 392.

626 UK Home Office, 'INTERCEPTION OF COMMUNICATIONS, Code Of Practice' Pursuant to Schedule 7 to the Investigatory Powers Act 2016) (2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

627 GDPR, art 23(1)(e).

628 APEC Privacy Framework, Part I, para 18.

629 APEC Privacy Framework, Part I, para 18.

630 ASEAN DP Framework, para 4.

631 OECD Guidelines, Chapter 1, Part 1, para 4.

In the HIPCAR Privacy Framework, data controllers can be exempt from complying with any provisions in the framework through an order published in the gazette in the interest of national security. Controllers who are public authorities are also exempt from compliance with rights and obligations under the framework, for data processing that is required for the prevention or detection of crime and other specified reasons. Similarly, personal data that is processed for discharging regulatory functions based on written laws are also exempted from these requirements.⁶³²

Notably, none of the frameworks exempt government bodies or public agencies from the obligation to impose adequate security safeguards for data that is collected and stored. These include technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data, such as the maintenance of adequate network security, putting in place authorisation and authentication measures, as well as providing device security. The OAS Principles also require that Member States refrain from requesting personal data collected by humanitarian organisations, noting that such data collection could be detrimental to humanitarian operations and the safety of the beneficiaries of such aid.⁶³³

“States must take care to narrowly define exemptions from data protection laws in their domestic legislation, and limit actions that can be undertaken pursuant to such exemptions”

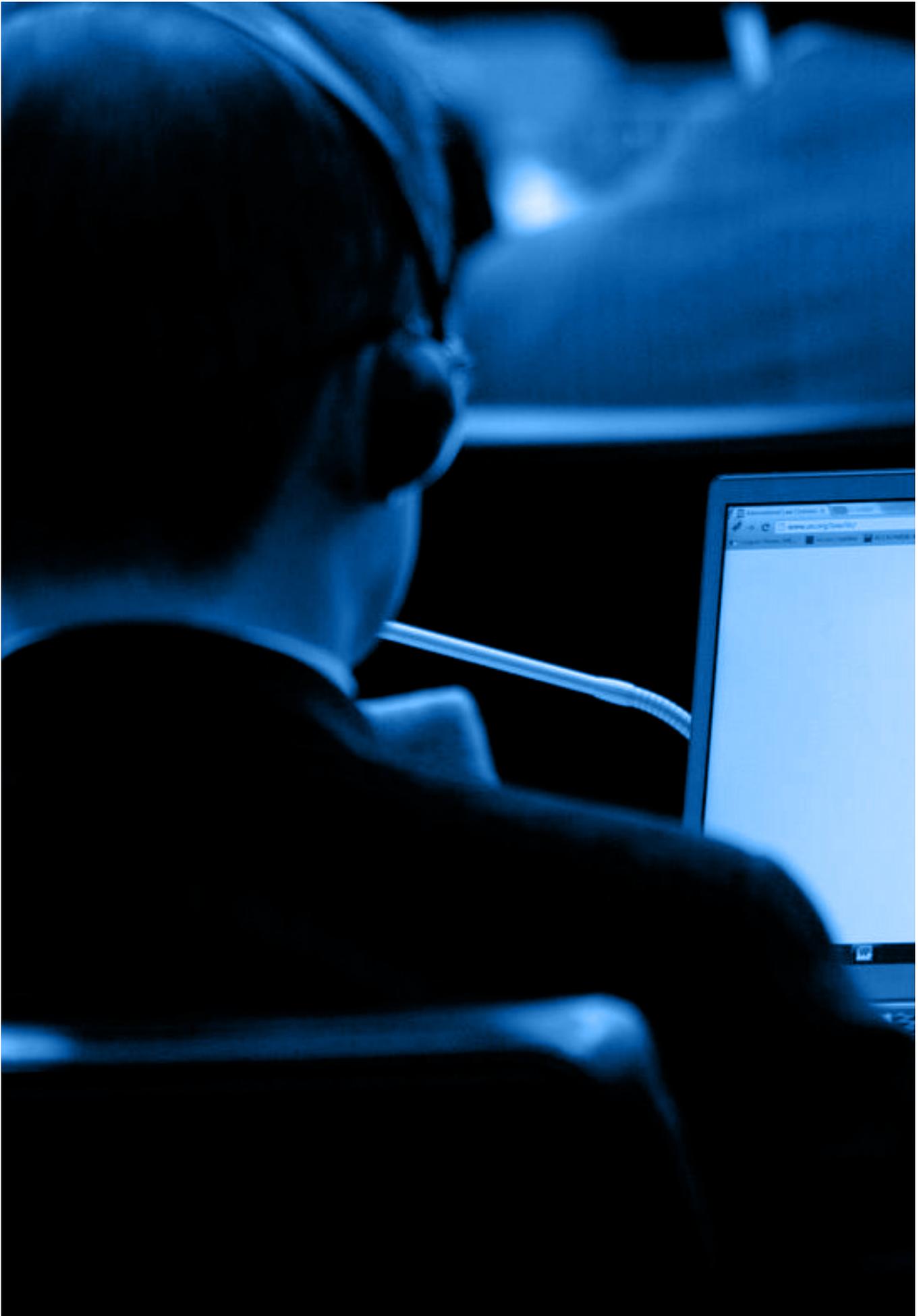


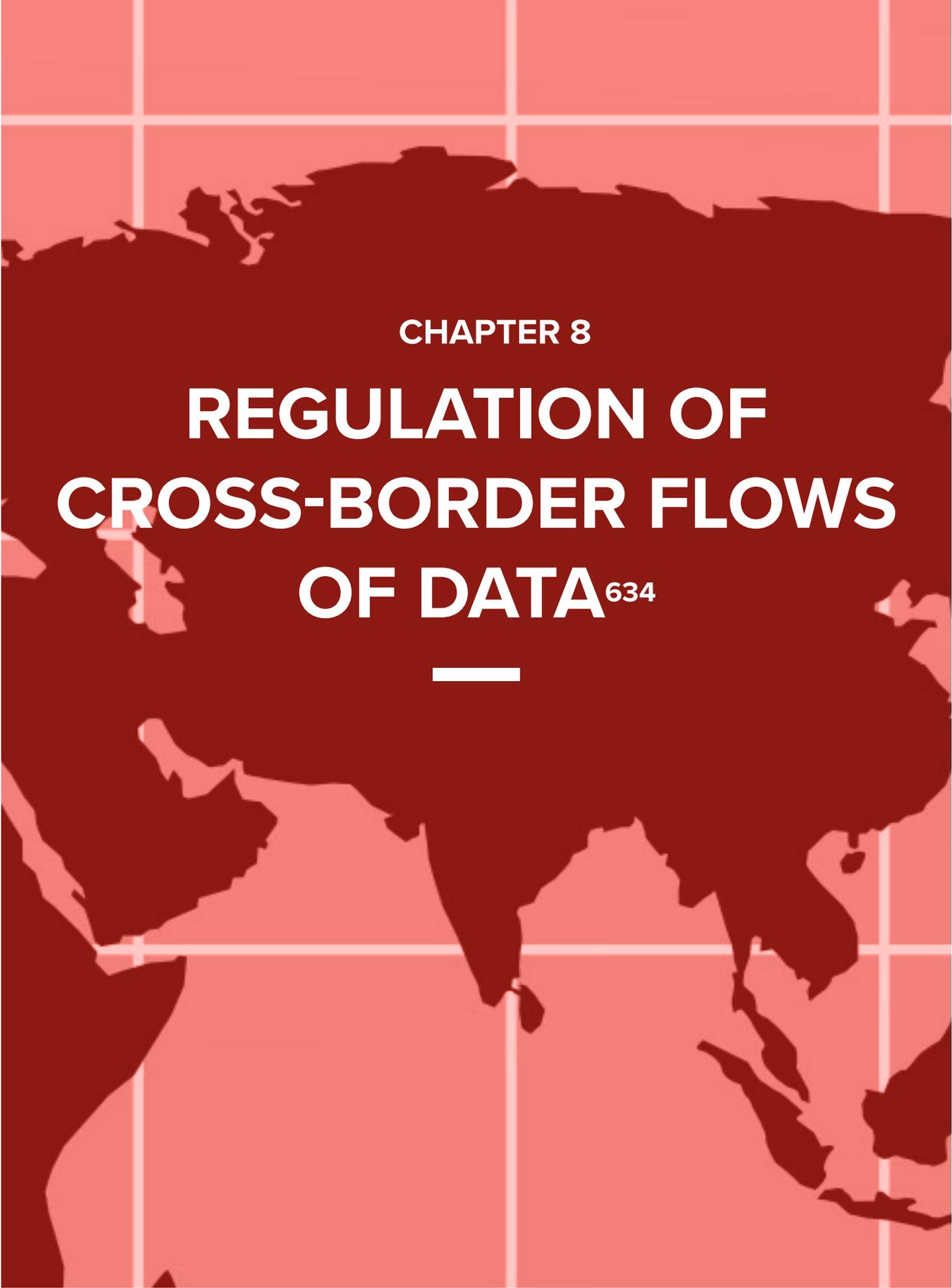
632 HIPCAR Model Legislative Texts, ss 35 and 36.

633 OAS Principles with Annotations, Principle 12, p 26.

Key considerations

- ◇ Government access and collection of data is sometimes necessary to pursue aims such as investigating crimes and upholding national security. To protect individuals against risks to the right to privacy, however, data protection laws provide adequate safeguards and regulate the collection and use of personal data by governments in accordance with data protection principles.
- ◇ International and national jurisprudence generally requires that restrictions on the right to privacy must be provided by law, not be arbitrary, pursue a legitimate aim, and be necessary and proportional to achieving a legitimate aim. International as well as domestic instruments and case law provide guidance on what each of these factors would entail.
- ◇ Frameworks studied in this report and national legislation typically exempt states and their agencies from compliance with data protection laws for reasons such as national security, the investigation of crimes, and the performance of regulatory functions. The obligations that states are exempted from vary, though the frameworks do not exempt states from the requirement to impose adequate data security safeguards.
- ◇ States must take care to narrowly define exemptions from data protection laws in their domestic legislation, and limit actions that can be undertaken pursuant to such exemptions. The exemptions must also be set out in the relevant legislation and be easily accessible, in order to hold government agencies accountable for the use of personal data and protect democratic freedoms.





CHAPTER 8

REGULATION OF CROSS-BORDER FLOWS OF DATA⁶³⁴

⁶³⁴ Restricted to aspects of cross-border data transfers that are typical to data protection frameworks and not issues like data sharing for criminal investigation.

8.1 Introduction

Regulation of cross-border flow of personal data has emerged as a critical aspect to consider within contemporary data protection legislation. At its core, this regulation reflects a constant tension between the need for seamless internet data flows and governments' 'legitimate need' to protect citizen's privacy and prevent data misuse.

This tension has resulted in several legislative and policy proposals around the world. With more than 200 countries either having adopted or proposing to adopt regulations pertaining to cross-border transfer of personal data,⁶³⁵ such laws either restrict international transfer of personal data through “conditional data flow regimes” or create frameworks which impose additional obligations on data controllers to localise personal data.⁶³⁶ Additionally, these laws impose obligations on data controllers to follow certain safeguards to ensure that personal data transferred abroad is secure and protects the privacy of the data subject.

The chapter holistically highlights a possible distinction emerging between data localisation policies and more traditional principles underlying the regulation of personal data flowing across borders in regions such as the EU. Data localisation creates an obligation on data controllers to store or host personal data, either partially or exclusively, within domestic borders. While regulatory triggers for data localisation are often contextual and unique to regional or national needs, a general criticism has gained significant momentum in global discourse that such models create cumbersome or unfeasible data

transfer requirements.

Furthermore, the diversity of laws and evolving policies on cross-border data flows has also given rise to concerns about potential fragmentation of the internet and global data processing activity.⁶³⁷ Explicit enactments by several countries of partial or exclusive personal data ‘localisation’ has been identified as being prejudicial to global business models contingent on data transfer, thus affecting investments and growth of the digital economy.⁶³⁸ A policy paper by the European Centre for International Economic Policy (ECIPE), highlights that such localisation requirements by proposed or enacted legislation could reduce GDP by 0.4 percent in the EU and Korea, 0.2 percent in Brazil, 0.1 percent in India. If applied to all sectors of the economy, it projects that the EU and Korea would see a decline of 1.1 percent in GDP and 0.8 percent in Brazil and India.⁶³⁹

This chapter highlights some of the key objectives for provisions that regulate cross-border data flows in proposed or existing legal frameworks. It discusses features of the Identified Regional Frameworks to showcase aspects taken into consideration while regulating such flows of data.

635 F. Casalini and J. López González, ‘Trade and Cross-Border Data Flows’ (2019) OECD Trade Policy Papers 220/2019, OECD Publishing, Paris <https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1635245466&id=id&accname=guest&checksum=22994166573CFAE848538C8DF256BF0D>.

636 Nigel Cory, ‘Cross-border data flows: Where are the barriers, and what do they cost?’ (Information Technology and Innovation Foundation, 1 May 2017) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>; Martina F. Ferracane, ‘Restrictions on Cross-Border data flows: a taxonomy’ (2017) EPICE Working Paper 1/2017 <https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf>.

637 UNCTAD, ‘Data protection regulations and international data flows: Implications for trade and development’ (2016), 32 https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf.

638 Coalition for Cross-border Data Flows, (July 2014) <https://aicasia.org/wp-content/uploads/2017/06/Data-Resource-Paper-July-3-1.pdf>.

639 European Centre for International Economic Policy, ‘The Costs of Data Localization: Friendly Fire on Economic Recovery’ (2014) https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf.

8.2 Regulatory objectives and origins of cross-border data flows

There are several regulatory objectives that underpin legislative proposals pertaining to cross-border flows of data. Key among these is the need to ensure that the country to which personal data is being transferred to provides a reasonable or comparable level of privacy protection and data security.⁶⁴⁰ These regulatory objectives emanate from the need to preserve fundamental rights and freedoms enjoyed by data subjects in the country of origin. In other cases, such objectives presumably serve to prioritise business or commercial interests to ensure seamless access to data in order to meet business and service needs.⁶⁴¹ Advocates of laws furthering cross border data flows argue that regulated transfers are likely to promote innovation and foster trade by domestic or homegrown businesses and data controllers.⁶⁴² Lastly, emerging regulations regarding international data transfer or localisation also seek to battle anti-competitive practices by big tech corporations and address concerns associated with national security and digital foreign interference.⁶⁴³

Academics and experts have criticised some of the abovementioned regulatory objectives and advocated for cross-border data flow models which are interoperable, adaptive to evolving data processing technology, and enable global digital trade.⁶⁴⁴ It is often argued that data decentralisation across national or regional borders is necessary to not only promote innovation, but also to enhance cybersecurity.⁶⁴⁵ This is especially important to avoid risks of data stores becoming an attractive target for potential security breaches.⁶⁴⁶ Furthermore, smooth and seamless cross-border data flows are critical to digital trade, communication, research, and service delivery across sectors such as finance, health, and education. This seamlessness of data flows is a vital component of business models for corporate entities across the world⁶⁴⁷ and several calls have been made to create frameworks that promote or negotiate interoperability among regional privacy frameworks.⁶⁴⁸

640 GDPR, Recital 101.

641 Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (2011), OECD Digital Economy Paper 187/2011, page 7 <http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf>.

642 Coalition for Cross-border Data Flows, July (2014) page 2 <https://aicasia.org/wp-content/uploads/2017/06/Data-Resource-Paper-July-3-1.pdf>.

643 Idris Ademuyiwa and Adedeji Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa' (2020), CIGI Papers 244/2020, page 7 https://www.cigionline.org/sites/default/files/documents/no244_0.pdf.

644 Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (Information Technology and Innovation Foundation, 19 July 2021) page 18 <https://www2.itif.org/2021-data-localization.pdf>; The UNDP Global Centre for Technology, Innovation and Sustainable Developme, 'Enabling Cross-Border Data Flow: ASEAN and Beyond', page 14 https://www.undp.org/sites/g/files/zskgke326/files/migration/sgtechcentre/Cross-border_data_flows_complete_report_UNDP.pdf.

645 BSA, 'Cross Border Data Flows' (2017) https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf.

646 Anupam Chander, Uyen P. Le, 'Breaking the Web: Data Localization vs. the Global Internet' (2014). Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper No. 378, Page 32 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

647 BSA, 'Cross Border Data Flows' (2017) https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf.

648 Idris Ademuyiwa and Adedeji Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa' (2020), CIGI Papers 244/2020, page 7 https://www.cigionline.org/sites/default/files/documents/no244_0.pdf;

One of the first regulatory formulations with regards to cross border data flows can be identified in the 1980 OECD Guidelines, which was subsequently updated in 2013. The OECD Guidelines define ‘transborder flows of personal data’ as ‘movements’ of personal data across ‘national borders.’⁶⁴⁹ The Guidelines acknowledge that Member States should avoid restricting flows of personal data if the receiving country adheres to the OECD Guidelines, or if sufficient safeguards exist to ensure a continuing level of protection.⁶⁵⁰ A similar principle allowing free cross-border flows to a country offering ‘comparable safeguards’ for privacy protection was also recognised by the United Nations General Assembly in its 1990 Guidelines for the Regulation of Computerized Personal Data Files.⁶⁵¹ In Europe, the regulatory origins on cross-border data flows are found in the 1981 Council of Europe’s Convention for the Protection of Individuals with regard(s) to Automatic Processing of Personal Data, otherwise known as Convention 108.⁶⁵² As the first binding international instrument pertaining to data protection and the regulation of transborder personal data flows, Convention 108 laid down certain principles and derogations for transborder data flows among parties to the Convention. This legal instrument was modernised in 2018 with the amended instrument referred to as Convention 108+, which directs states against placing a blanket prohibition on the transborder flow of personal data for the purposes of protecting personal data.⁶⁵³ Parties to the Convention are permitted to derogate in specific instances, such as when there is a risk that a transfer (to treaty-parties, or from another treaty-party to a non-Party) would circumvent the Convention’s provisions.⁶⁵⁴



649 Organisation for Economic Co-Operation and Development, 'The OECD Privacy Framework' (2013), Chapter 1, Part 1, para 1(e) www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

650 OECD Guidelines, Chapter 1, Part 4, para 17.

651 UN General Assembly, 'Guidelines for the Regulation of Computerized Personal Data Files' (14 December 1990) <https://www.refworld.org/docid/3ddcafaac.html>.

652 Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (1981) ETS 108 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>;

653 Convention 108+, art 14; While Convention 108 is binding, Convention 108+ which an amending protocol is not binding; Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (final dated 18 May 2018) CETS No. 223 <https://rm.coe.int/16808ac918>.

654 Convention 108+, art 14(1).

The need to balance privacy protections with seamless data flows has been explicitly recognised by binding and non-binding privacy clauses in regional and international instruments which underscore the responsibility to ensure reasonable restrictions while maintaining seamless data flows. For instance, the OECD Guidelines acknowledge that restrictions may be imposed, but such restrictions should not be disproportionate to the risks presented.⁶⁵⁵ Some regional frameworks, such as the GDPR, have retained a similar approach⁶⁵⁶ while expanding the duties and obligations of Member States and data controllers, and have adopted a 'layered approach' to international data transfers. This involves examining if the third country affords an adequate level of protection, and if not, the data exporter takes it upon themselves to provide the necessary safeguards to ensure protection in the third country.⁶⁵⁷ Similarly, the APEC Privacy Framework, while making an explicit recognition of the need to protect data subject interests during cross-border flows of data, warns against the imposition of "unnecessary barriers to information flows."⁶⁵⁸

These principles are also echoed in existing and emerging privacy frameworks across the globe and are included in most Identified Regional Frameworks.⁶⁵⁹ Furthermore, while some instruments, such as the APEC Privacy Framework, have been considered less stringent than the EU model due to their voluntary nature, scholars have argued that no single framework is likely to provide a complete solution to address the challenges of cross-border data flows and that 'incremental answers' will continue to evolve through global dialogue.⁶⁶⁰

The following sections examine some notable features of the Identified Regional Frameworks, with regards to the regulation of cross-border personal data transfers, and also identify evolving global practice for same.

"...no single framework is likely to provide a complete solution to address the challenges of cross-border data flows and that 'incremental answers' will continue to evolve through global dialogue"

655 OECD Guidelines, Chapter 1, Part 1, para 18.

656 Paul Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 HLR http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf.

657 Art 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (2005) WP 114, 9 https://www.datatilsynet.dk/media/7876/wp114_en.pdf.

658 APEC Privacy Framework, para 36, part iv.

659 African Union's Convention on Cyber Security and Personal Data Protection ('AU Convention'), the HIPCAR Model Policy Guidelines and Legislative Text ('HIPCAR Privacy Framework'), the APEC Privacy Framework, the ASEAN Framework on Personal Data Protection ('ASEAN DP Framework'), and the Organisation of American States' Principles on Privacy and Personal Data Protection ('OAS Principles')

660 Clare Sullivan, 'EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era' (2019) 35 CLSR 4 <https://www.sciencedirect.com/science/article/abs/pii/S026736491930038X>; Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014), 4; Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (2011), OECD Digital Economy Paper 187/2011 <http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf>.

8.3 Adequacy and conditions for transfer permitting cross-border data flows

8.3.1 Adequacy within Identified Regional Frameworks

Transfer of personal data to another country or territory is often subject to the prevailing laws and protections afforded by the destination country or by those followed by the data controller responsible for the transfer. The existence of an adequate level of data protection as a prerequisite for cross-border flows can be found in the ASEAN DP Framework, HIPCAR Privacy Framework, AU Convention, and the GDPR.⁶⁶¹ In these regional and other national⁶⁶² frameworks, personal data transfers should be made on the basis of a subjective decision - by the relevant authority such as a Data Commissioner - on reciprocity, adequacy or the existence of 'comparable safeguards' associated with data protection.⁶⁶³

The adequacy principle rooted in the 1995 EU Data Protection Directive, and currently embedded in the GDPR, has significantly influenced the EU's data protection regime and global privacy frameworks.⁶⁶⁴ While these terms and phrases such as reciprocity and adequacy have not been explicitly defined in law, they involve assessing certain elements that determine the existence of a comparable or a reasonable level of data protection in the third country, territory, or international organisation where personal data is being transferred to. In this context, a

third country refers to a country outside the European Economic Area (EEA). The European Commission, in such cases, may decide that the third country or territory (or certain sectors in that country) or an international organisation "ensures an adequate level of protection."⁶⁶⁵ When considering particular sectors in determining adequacy levels, the implementing act may specify sectoral application of the act.⁶⁶⁶

Similarly, adequacy (in the case of the AU Convention) can be understood as an "adequate level of protection of the privacy, freedoms and fundamental rights" for data subjects.⁶⁶⁷ The OAS Principles also outline a framework for the international transfer of personal data. According to the OAS Principles, personal data can be transferred internationally if the data controller is responsible for ensuring that the information is protected. They also provide that the destination state should offer a degree of personal data protection which is in accordance with the standards set out in the Principles, if the personal data is being transferred internationally.⁶⁶⁸ Thus, the OAS Principles also echo the adequacy principle located in other instruments. The ASEAN Privacy Framework outlines two conditions for the international transfer of personal data. The 'organisation' transferring the data should either obtain the consent of the data subject for a transfer, or ensure that the receiving organisation protects the personal data in accordance with the principles of the ASEAN Privacy Framework.⁶⁶⁹

661 GDPR, art 45; African Union Convention on Cyber Security and Personal Data Protection (27 June 2014), art 14 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf; HIPCAR, Model Legislative Text, s 7(h) http://caricom.org/documents/16583-privacy_and_data_protection_mpg.pdf; ASEAN Telecommunications and Information Technology Ministers Meeting, 'Framework On Personal Data Protection' (16 November 2016), Principle 6(f) <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>.

662 International Conference of Data Protection and Privacy Commissioners (5 November 2009), chapter 15 <https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf>; The Data Protection Bill, 2021 (India), The Privacy Amendment Act (Australia), The Personal Information Protection and Electronic Documents Act (Canada)

663 HIPCAR Model Legislative Text, s 19; AU Convention, art 10(6)(k); Internet Society and the Commission of the African Union, 'Personal Data Protection Guidelines for Africa' (9 May 2018) https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.

664 UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' (2016), page 32 https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf.

665 GDPR, art 45(1).

666 GDPR, art 45(3)

667 AU Convention, art 14(6)(a).

668 OAS Principles with Annotations, principle 11, page 23, 24.

669 ASEAN DP Framework, principle 6(f).

It can be observed that regional frameworks such as the GDPR and the AU Convention have adequacy standards for personal data transfer outside the region or to non-member/participating countries that are higher than standards for transfer within the region the framework applies to. Models such as the GDPR provide for specific and contextual adequacy assessments for nations, regions, international organisations, or other specific sectors. Furthermore, all the regional frameworks examined for the purpose of this chapter designate national or regional regulatory bodies or data protection regulators to authorise and govern cross-border personal data transfers. For instance, regulators such as the National Data Protection Authorities (AU Convention) or Data Commissioners (HIPCAR Privacy Framework) are responsible for managing authorisations pertaining to cross-border personal data transfer.⁶⁷⁰ In the case of the GDPR, the European Commission is tasked with the responsibility of making such assessments pursuant to Article 45. Both frameworks also incorporate respect for fundamental rights and freedoms into adequacy assessments.⁶⁷¹

8.3.2 Factors determining adequacy

Regional frameworks provide an exhaustive list of factors to be considered by relevant authorities when making an assessment for adequacy. For instance, the HIPCAR Privacy Framework provides that to make an adequacy assessment for a receiving country, authorities shall examine factors such as the ‘nature of data,’ the countries or jurisdictions involved in the personal data transfer, the nature, purpose, and duration of processing, and the existence of ‘security measures’ for the transfer.⁶⁷²

The GDPR’s Article 45 outlines key considerations that the European Commission needs to follow when making an adequacy assessment. These are as follows: (i) the existing legislative framework and rule of law in the receiving country; (ii) the existence of “data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country;” (iii) the existence of an independent and



functional supervisory authority, and; (iv) international agreements or commitments adopted by the country or international organisation, including ‘legally binding conventions or instruments’ or ‘multilateral or regional systems’ associated with personal data protection.⁶⁷³

8.3.3 Transparency, consultation, and monitoring of adequacy assessments

Laws like the GDPR envisage adequacy assessments to be dynamic and are subject to periodic monitoring. Once a decision on adequacy has been made by the European Commission, the implementing instrument must provide for a “mechanism for periodic review.” Such reviews should take into account ‘relevant’ developments in the third country or international organisation. Furthermore, the Commission is also required to regularly monitor any developments in the country or organisation which may affect the adequacy decision.⁶⁷⁴

670 AU Convention, art 12(2)(k); HIPCAR Model Legislative Text, s 19(3); GDPR, art 45(1).

671 AU Convention, art 14(6)(a); GDPR art 45(2)(a).

672 HIPCAR Model Legislative Text, s 19(2).

673 GDPR, art 45(2)(a), (b), (c); Rule of law is also a factor for consideration for adequacy in the HIPCAR Privacy Framework, HIPCAR Model Legislative Text, s 19(2).

674 GDPR, art 45(3), (4); GDPR Recital 106.



In the context of making decisions on adequacy, the GDPR also lays down critical transparency obligations for the European Commission, such as the publication, on its website, of ‘whitelisted’ third countries, sectors, or international organisations. When considering adequacy levels for particular sectors especially, the GDPR states that an implementing act may specify the extent to which adequacy requirements relate to a sector.⁶⁷⁵ The Commission is also obliged to provide details on sectors or entities which fail to satisfy the adequacy requirements. In instances where the Commission is of the opinion that an adequate level of protection is “no longer ensured,” it shall consult the concerned entities in order to address the situation.⁶⁷⁶

A similar transparency standard for cross border data flows has not been encoded in the other Identified

Regional Frameworks. However, these and existing and evolving national frameworks have been explored below to further understand standards for transparency, monitoring, and decision-making for cross-border data flows.

8.3.4 Deemed adequacy – The development of the EU-US ‘Privacy Shield’

Most regional frameworks have incorporated varying standards of adequacy to assess cross-border data flows. So far, existing GDPR practice lays down an exhaustive standard to carry out adequacy assessments for non-EU countries, international organisations and other sectors. However, the GDPR permits specific and contextual transfers in cases when a nation is not deemed adequate for the purpose of blanket transfers without safeguards. Consequently, in the absence of adequacy requirements, certain industries may proceed with international transfer of personal data through a self-certification mechanism which is deemed adequate.

The EU-US Privacy Shield, which is no longer in effect, is an important illustration of this mechanism. Initially preceded by the ‘Safe Harbour’, personal data transfers from the EU to the US were permitted pursuant to safeguards adhered to by American private organisations and data controllers.⁶⁷⁷ The Safe Harbour was imposed to ensure that personal data processed by organisations in the United States and the European Union remained protected. It outlined seven compliance principles for companies which consisted of notice, choice, onward transfer, security, data integrity, access and enforcement.⁶⁷⁸ However, this arrangement was declared invalid in 2015 by the ECJ as a result of the *Schrems v Data Protection Commissioner* case (Schrems I).⁶⁷⁹ The court noted that a self-certification system might adhere to an adequate level of protection in accordance

⁶⁷⁵ GDPR, art 45(3)

⁶⁷⁶ GDPR, art 45(6); art 45(8), (6); European Commission, ‘Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection’ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

⁶⁷⁷ Pankaj Maru, ‘From Safe Harbour to Privacy Shield to GDPR: the journey of data protection laws’ (The Economics Times, 26 May, 2018) <https://cio.economictimes.indiatimes.com/news/government-policy/from-safe-harbour-to-privacy-shield-to-gdpr-the-journey-of-data-protection-laws/64327558>.

⁶⁷⁸ Federal Trade Commission, ‘Enforcement of the US-EU and US-Swiss Safe Harbor Frameworks’ <https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor>.

⁶⁷⁹ Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] EU:C:2015:650 <https://privacylegistry.org/case/maximilian-schrems-vs-data-protection-commission>.

with a third country's domestic law. However, the 'reliability' of such a system should fundamentally be based on the existence of "effective detection and supervision mechanisms" in the destination country. Such mechanisms would have to identify and punish infringements of rules relating to the right to privacy and personal data protection.⁶⁸⁰

The European Commission subsequently assessed the limitations and safeguards available in US laws which led to the replacement of the Safe Harbour with the Privacy Shield. The Privacy Shield Principles were issued by the US Department of Commerce to "foster, promote, and develop" international commerce and ensure the protection of EU data subjects. Among other things, the Privacy Shield Principles put in place stronger obligations related to the self-certification mechanisms for companies and mandatory cooperation with Data Protection Authorities when processing certain categories of data. Redress mechanisms for non-compliance were also introduced.⁶⁸¹

The ECJ, however, on July 16 2020, in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*⁶⁸² (Schrems II), invalidated the Privacy Shield while reviewing the Privacy Shield and standard contractual clause (SCCs) arrangements between the EU and US. This was due to critical gaps in US law that permitted surveillance agencies to access EU data subjects' information for national security investigations. The ECJ, however, noted that Standard Contractual Clauses could be used as an alternative data transfer mechanism to ensure compliance. However, data controllers who intend to use SCCs to transfer data are legally required to carry out an assessment of whether US law provides adequate protections which should be in accordance with EU law. If they cannot guarantee compliance with the SCCs, they cannot use it. In such circumstances, data controllers will have to identify supplementary measures to ensure compliance.⁶⁸³ Data transfers to

the US can also be made under certain circumstances such as data subject consent or contractual performance as provided for in the GDPR's Article 49, which is applicable in cases where no adequacy decision is made for that country.⁶⁸⁴ The European Commission revised SCCs shortly after Schrems II, dividing the instruments into two categories of use. One is for use between data controllers and processors within the EEA, and the other for transfers to third countries.⁶⁸⁵ In March 2022, the European Commission and the United States agreed in principle on a new Trans-Atlantic Data Privacy Framework that addresses concerns raised in Schrems II.⁶⁸⁶

680 Schrems I, para 81.

681 EU-US Privacy Shield Framework Principles, section III, principle 6 <https://www.privacyshield.gov/EU-US-Framework>; European Parliamentary Research Service (EPRS), 'From Safe Harbour to Privacy Shield' [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA\(2017\)595892_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf).

682 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems [2020] ECLI:EU:C:2020:559.

683 Schrems II, para 133.

684 Schrems II, para 201, 202.

685 European Commission, 'Standard Contractual Clauses (SCC)' (4 June 2021) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

686 European Commission, 'European Commission and United States Joint Statements on Trans-Atlantic Data Privacy Framework' (25 March 2022) https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087.

8.4 Obligations on data controllers and accountability

8.4.1 Appropriate safeguards and organisational responsibility

In the absence of a decision on adequacy, personal data may be transferred to another country subject to certain safeguards and obligations.

The GDPR outlines certain ‘appropriate safeguards’ for such transfers to take place, and further obligates data controllers to ensure that ‘enforceable data subject rights’ and ‘effective legal remedies’ are present.⁶⁸⁷ According to the GDPR, these safeguards can be in the form of legally binding instruments only between public authorities or bodies within the EEA to those in third countries/international organisations; these safeguards do not include transfers involving any private entity.⁶⁸⁸ They can also include Binding Corporate Rules (BCRs) and Standard Data Protection Clauses (SDCs).⁶⁸⁹ Other safeguards include approved codes of conduct with “binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards.”⁶⁹⁰ Alternatively, an approved certification mechanism along with a commitment to comply with appropriate safeguards which protect data subject rights, can also act as a safeguard.⁶⁹¹ In such instances, the GDPR stipulates that specific permissions from ‘supervisory authorities’ are not required.

The following subsections explore two key GDPR safeguards, namely the Standard Contractual Clauses associated with data protection, and the Binding Corporate Rules. While similar arrangements cannot be immediately identified in other frameworks, these

safeguards have emerged as accepted global best practice for organisational transfer of personal data across borders. They may be useful in ensuring accountable and protected transfers of personal data by data controllers and processors.

8.4.1.1 Standard Contractual Clauses

In the absence of a decision on adequacy or the existence of a comparable framework for data protection, the European Commission can, through instruments such as the GDPR, recognise SCCs which contain adequate safeguards and protections for personal data to be transferred internationally. These are model clauses on data security and privacy protection that are approved by the European Commission and can be incorporated and implemented by data controllers or processors. The European Commission has issued modernised SCCs for transfer of data to data controllers and processors established outside the EU/EEA that reflect the GDPR and the implications of Schrems II.⁶⁹²

8.4.1.2 Binding Corporate Rules – Obligations for multi-national corporations

According to the GDPR, a BCR refers to “personal data protection policies” which are implemented by data controllers or processors “established on the territory of a Member State” for situations which entail personal data transfers to data controllers or processors in one or more countries, but within a “group of undertakings, or group of enterprises engaged in joint economic activity.”⁶⁹³ BCRs are approved by national supervisory authorities based

687 GDPR, art 46; GDPR, Recital 108.

688 EDPB, ‘ Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies’ (18 January 2020) https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf.

689 GDPR, art 46(2)(a), (b); GDPR, Recital 109

690 GDPR, art 46(2)(e), in accordance with the provisions laid down in GDPR, art 40.

691 GDPR, art 46(2)(f), in accordance with the provisions laid down in GDPR, art 42.

692 European Commission, ‘Standard contractual clauses for data transfers between EU and non-EU countries’ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

693 GDPR, art 4(20); GDPR, Recital 110.

on certain conditions laid down in the GDPR.⁶⁹⁴

Such BCRs should;⁶⁹⁵

- contain necessary information and disclosures associated with the data transfer;
- identify the data controllers or processors and the group of undertakings or enterprises;
- describe the nature and extent of data protection principles being complied with;
- include complaint procedures;
- provide mechanisms for “reporting and recording changes to the rules.”

Furthermore, the law imposes a duty on the European Commission to formulate appropriate procedures for BCR associated information exchange between data controllers and processors and the concerned supervisory authorities.

The above-mentioned safeguards outlined in regional frameworks such as the GDPR provide a glimpse of binding security safeguards that must be implemented by data controllers and organisations. There also exist alternative non-binding models of accountability and data security outlined in some of the other Regional Identified Frameworks. The ASEAN Digital Governance Framework contains Model Contractual Clauses for Cross Border Data Flows which are a voluntary standard of terms and conditions that may be included in binding legal agreements between parties. While the clauses are designed for the purpose of transfers within the ASEAN region, the framework provides parties the flexibility to use these clauses with appropriate modifications based on their own discretion.⁶⁹⁶

The OAS Principles, for instance, require that obligations of a data controller should be recognised through appropriate agreements, contractual provisions or even within technical and organisational security safeguards.⁶⁹⁷ The APEC Cross-Border Privacy Rules (CBPRs) are an excellent illustration of a ‘government-backed’ privacy certification.⁶⁹⁸ The

CBPRs provide a flexible and voluntary framework for APEC Member States to adopt a minimum standard for data protection, which includes enforceable standards, risk-based protections, and consumer friendly grievance redressal mechanisms.⁶⁹⁹

694 GDPR, art 47(1).

695 GDPR, art 47(2)(a), (b), (d), (i), (k)

696 ASEAN Digital Governance Framework, Model Contractual Clauses for Cross Border Data Flows, page 4 https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

697 OAS Principles with Annotations, Principle 11, page 26.

698 ‘What is Cross-Border Privacy Rules System?’ (APEC, 15 April 2019) <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>.

699 Andrei Gribakov, ‘Cross-Border Privacy Rules in Asia: An Overview’ (Lawfare, 3 January 2019) <https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview#:~:text=Thus%2C%20the%20CBPR%20system%20is,data%20flows%20across%20national%20borders.&text=However%2C%20because%20the%20CBPR%20system,that%20set%20a%20stricter%20standards>.

8.5 Derogations, exceptions, and specific grounds for transfer in place of adequacy

There are certain exceptions or circumstances in which adequacy requirements may be bypassed when transferring personal data to another country or organisation. Varying standards of these exceptions may be found in the Identified Regional Frameworks such as the GDPR, the OAS Principles, the HIPCAR Privacy Framework, the ASEAN DP Framework, and the AU Convention. The existence of such derogations or exceptions may appear to be opportunities to bypass critical adequacy assessments or compliance with extensive safeguards and make it “substantially easy” for data controllers to transfer data to third countries. However, these exceptions do not, by themselves, absolve data controllers of the responsibility to protect the personal data being transferred. Instead, they provide flexibility for data controllers in situations where transfer is essential to serve the interests of the data subject or to support important public interest objectives. An explanation for allowing certain conditions to exist may come from efforts to facilitate efficient international data transfers for trade and business activity. For example, circumstances where data transfers might be necessary to fulfil contractual agreements. In several instances, such derogations or additional grounds are to be narrowly interpreted to ensure that the “exception does not become the rule.”⁷⁰⁰

The following sections explore common derogations and exceptions in the Identified Regional Frameworks.

8.5.1 Consent of data subject

In some circumstances, the cross-border transfer of personal data is permitted when consent is provided by the data subject. For instance, according to the GDPR, personal data may be transferred to a third country or an international organisation in the absence of an adequacy decision or appropriate safeguards, if the data subject “explicitly consents to the proposed transfer.”⁷⁰¹ However, a data subject’s mere consent is not the only criteria that facilitates a data transfer to take place in such situations. The GDPR stipulates that such consent would be considered meaningful only if the data subject has been “informed of the possible risks of such transfers.”⁷⁰²

The GDPR standards of consent for personal data transfer have evolved considerably when compared to the EU’s Data Protection Directive. The GDPR now provides for explicit consent and reflects a significant deviation from the EU Data Protection Directive’s requirement for a relatively lower standard of unambiguous consent.⁷⁰³ It should be pointed out that the GDPR states that consent as a condition for personal data transfer shall not be applicable to activities carried out by public authorities “in the exercise of their public power.”⁷⁰⁴

Meanwhile, the HIPCAR Privacy Framework also outlines data subject’s consent as grounds for a limited form of transfer of personal data in the absence of adequacy. It allows for such a transfer to take place if the Data Commissioner determines that it can be done in a manner that would limit the breach of the data subject’s rights.⁷⁰⁵

700 Article 29 Working Party, ‘Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995’ (2005) WP 114, 7, cited in Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (2018), EDPB https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf; Additional Protocol to Convention 108 on the control authorities and crossborder flows of data (2001) ETS 181, art 2(2)(a) <http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm>.

701 GDPR, art 49(1)(a); GDPR, art 46.

702 GDPR, art 49(1)(a); EDPB, ‘Guidelines 05/2020 on consent under Regulation 2016/679’ (4 May 2020) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

703 GDPR, art 49(1)(a); Article 29 Working Party, ‘Opinion 15/2011 on the definition of consent’ (13 July 2011) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf;

704 GDPR, art 49(3).

705 HIPCAR Model Legislative Text, s 19(4), page 25.

8.5.2 Contractual necessity

In instances where a receiving country's laws are deemed to be inadequate for the purpose of personal data protection, transfers may be permitted if it is necessary to process such data to comply with a contract, or if the pre-contractual arrangements requested by the data subject compel data controllers or exporters to adhere to baseline norms of data protection. The test of necessity and ensuring that data transfers are "occasional" are key safeguards for this derogation that data exporters need to include in their assessments of data transfers. For instance, the GDPR allows for contractual necessity to be invoked as grounds for the transfer of personal data if a decision on adequacy has not been made or if appropriate safeguards provided for in Article 46 (transfers subject to appropriate safeguards) are not present. In such cases, personal data may be transferred if it is "necessary for the performance of a contract between the data subject and the data controller" or for the implementation of 'pre-contractual measures' which may take place at the data subject's request.⁷⁰⁶ It also stipulates that personal data may be transferred if it is necessary for the conclusion or performance of a contract "concluded in the interest of the data subject between the controller and another natural legal person."⁷⁰⁷ None of these provisions, however, are applicable to activities carried out by officials "in the exercise of a public power."⁷⁰⁸

8.5.3 Transfer necessary for public or vital interest or carried out by a public authority

Personal data may be transferred internationally if a data subject's life is at risk, where a data subject is physically or legally incapable of providing consent, or where a significant public interest objective has been invoked. The GDPR explicitly states that personal data may be transferred to a third country or an international organisation if it is necessary for "important reasons of public interest."⁷⁰⁹ However,

the GDPR also states that matters of public interest should be laid down in EU law or Member State law as applicable to the data controller.⁷¹⁰

Similarly, the OAS Principles also include an equivalent consideration where transfers of personal data are not restricted between humanitarian organisations and entities that provide humanitarian services. This is based on the reasoning that these organisations might need to engage in such transfers to safeguard the vital interests of data subjects or for the purposes of public interest.⁷¹¹

The GDPR's 'vital interest' condition accounts for public health outbreaks or emerging health situations whereby the health or life of the data subject may be at risk. Contemporary data protection laws take into account circumstances that make it practically unfeasible to obtain an adequacy assessment in a timely manner. In such cases, the "imminent risk of serious harm" outweighs privacy concerns. Such a derogation may also be enforced during natural disasters when the transfer of personal data is necessary for "rescue and retrieval operations"⁷¹² or pandemics or public health outbreaks when the cross-border flow of personal data is critical for health and safety responses.

For instance, the COVID-19 pandemic has prompted nations and private entities to develop contact-tracing applications, formulate plans for vaccine research, and gather data for effective medical and social responses. In some cases, data protection regulators have issued advisories and clarifications on data protection frameworks to ensure seamless data flow while also protecting the rights and interests of the data subjects involved. EU Agencies have been playing an active role in this context. Recognising the

706 GDPR, art 49(1)(b).

707 GDPR, art 49(3).

708 GDPR, art 49(1)(d).

709 GDPR, art 49(1)(d).

710 GDPR, art 49(1)(4).

711 OAS Principles with Annotations, Principle 11, page 24.

712 EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' (2018) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

need for measures to combat the COVID-19 pandemic as a public interest objective, the EU issued guidelines for data transfers when ‘strictly necessary.’⁷¹³ In 2020, the European Commission also set up an interoperability gateway service linking national contact-tracing applications across the EU to safely exchange information between the applications based on a decentralised architecture.⁷¹⁴ As part of this initiative, Member States involved adopted a toolbox with guidance for such contact tracing mobile applications which necessitate that these applications are privacy preserving.

8.5.4 Additional considerations and grounds for transfer

8.5.4.1 Restricted and redacted transfers

According to the HIPCAR Privacy Framework, a restricted data transfer may be permitted by the Data Commissioner when the receiving country does not have adequate or comparable levels of data protection to limit the breach of a data subject’s rights if the data subject consents to such transfer, and if critical aspects of the information are suitably redacted or removed.⁷¹⁵

8.5.4.2 Transfers in exercise or defence of legal claims

The GDPR permits cross-border flow of personal data in the exercise or defence of legal claims’ and when transfers are made from a “register which according to European Union or Member State law is intended to provide information to the public.” Additional safeguards are provided for in the law for the transfer of data in such situations.⁷¹⁶

8.5.4.3 Transfers in pursuance of a compelling legitimate interest

The GDPR also contains a residuary provision that permits transfer of personal data in the absence of an adequacy decision or appropriate safeguards in instances where the transfer is necessary for the purpose of a ‘compelling legitimate interest,’ and which does not offend the rights and freedoms enjoyed by the data subject.⁷¹⁷ In this scenario, a compelling legitimate interest would include situations when transfer is necessary for the performance of a contract, to support important public interest objectives and to protect the data subject’s vital interests.⁷¹⁸ In addition, such a transfer is only permitted when it is not repetitive and is associated with a limited number of data subjects.⁷¹⁹

The residual clause also places an obligation on the data controller to ensure the presence of sufficient safeguards to protect the personal data for such transfers, to provide necessary information to the ‘supervisory authority’, as well as to the data subject.⁷²⁰ The GDPR also states that in situations when an adequacy decision has not been made, EU or Member State laws may for important reasons of public interest, outline restrictions for the transfer of certain categories of personal data and that the European Commission be notified of these legal provisions.⁷²¹

713 EDPB, ‘Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak’ (2020) page 8, 12 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf; https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020-0030_mep_duris_covid19_en.pdf.

714 EU interoperability gateway goes live, first contact tracing and warning apps linked to the system’ (19 October 2020) https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904.

715 HIPCAR Model Legislative Text, s 19(4).

716 GDPR, art 49(1)(e), (g) and art 49(2).

717 GDPR, art 49(4); GDPR, art 49(1)(2).

718 GDPR, art 49(1)(b), (d), (f).

719 GDPR, art 49(1)(2).

720 GDPR, art 49(1)(2), art 49(6).

721 GDPR, art 49(5).



8.6 Non-compliance, sanctions and penalties

Some of the Identified Regional Frameworks outline specific offences and penalties for violations of the norms regulating cross-border information transfers. For instance, the HIPCAR Privacy Framework stipulates that transferring personal information without proper authorisation is a criminal offence and can attract imprisonment or a penalty.⁷²² The GDPR also includes penalties that subject an entity to “administrative fines up to 20,000,000 Euro” for violating the cross-border data flow provisions included

in Articles 44-49. In the case of an ‘undertaking’ the fine should for an entity represent as much as “4% of the total worldwide annual turnover.”⁷²³ Specific frameworks for offences and penalties for violating provisions of cross-border flows can also be located in domestic legislation.⁷²⁴

722 HIPCAR, Model Legislative Text, s 74.

723 GDPR, art 83 (5).

724 Report of the Joint Committee on the Personal Data Protection Bill, 2019, s 57(2)(d) available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf; Alexander Gurkov, Personal Data Protection in Russia (2021) The Palgrave Handbook of Digital Russia Studies, section 6.3.3; Rogier Creemers and Graham Webster, 'Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021' (DigiChina Stanford University, 20 August 2021) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

Box 8.1 - Data Transfer Mechanisms for Law Enforcement

For cross-border crimes, the transfer and sharing of personal data of individuals under investigation is critical to ensure efficient investigations.⁷²⁵ One of the ways in which such data has traditionally been shared is through Mutual Legal Assistance Treaties (MLATs), which are treaties or agreements between two or more countries that allow for law enforcement to cooperate, collect, and transfer information from one country to another in order to assist with the investigation of criminals.⁷²⁶ In cases where there are no MLATs, the traditional method of Letter of Request can be made by a court of law of one country to another.⁷²⁷ The G8 24/7 Cybercrime Network, which includes 80 countries, attempts to supplement and enhance these traditional methods of data sharing. This network allows for the preservation of electronic evidence by participating countries, as well as the sharing of information through MLATs or Letters of Request.⁷²⁸ The GDPR's Article 48 recognises these methods, but provides that an international transfer of personal data as requested by the courts or administrative authorities of a third country can only take place through international agreements like MLATs between the 'requesting third country' and the concerned EU Member State.

725 Peter Swire and Justin D Hemmings, 'Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program' (2016) 71 NYU Ann Surv Am L 687.

726 ICC Commission, 'Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures' (2012) Document No. 373/512 [https://www.icc-portugal.com/images/publicacoes/documentos_gratuitos/Economia_Digital/ICC_policy_statement_on_Using_Mutual_Legal_Assistance_Treaties_\(MLATs\)_To_Improve_Cross-Border_Lawful_Intercept_Procedures_\(2012\).pdf](https://www.icc-portugal.com/images/publicacoes/documentos_gratuitos/Economia_Digital/ICC_policy_statement_on_Using_Mutual_Legal_Assistance_Treaties_(MLATs)_To_Improve_Cross-Border_Lawful_Intercept_Procedures_(2012).pdf).

727 Philip F. Sutherland, 'The Use of the Letter of Request (Or Letter Rogatory) for the Purpose of Obtaining Evidence for Proceedings in England and Abroad' (1982) 31 The International and Comparative Law Quarterly 784 https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf.

728 Organization of American States, 'The G8 24/7 Network of Contact Points Protocol Statement' http://www.oas.org/juridico/english/cyb_pry_g8_network.pdf.

One of the concerns around traditional instruments such as MLATs is that they are time consuming and may impede critical law enforcement activity. Moreover, the request for data sharing may also be rejected.⁷²⁹ For this reason, many countries are opting for laws and policies that facilitate the direct and efficient cross-border sharing of personal data for law enforcement purposes, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act in the United States.⁷³⁰

In Europe, the EU Law Enforcement Directive (LED) consists of legislation that deals with the protection and free movement of personal data that is used for the investigation, detection or prosecution of criminal offences between relevant European authorities. The LED also provides that personal data must be processed only for the purposes mentioned in the directive, and in a manner that ensures security and confidentiality of the personal data.⁷³¹ In addition, it also provides for the rights of the data subject, such as access to the information that is being processed.⁷³² The GDPR and LED function in a complementary fashion to each other. While the GDPR provides for general rules regarding the protection and free movement of personal data, the LED focuses on the processing and movement of personal data for the purpose of criminal investigations and prosecution.⁷³³

729 Smriti Parsheera and Prateek Jha, 'Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?' (2020) Carnegie Endowment For International Peace https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf.

730 18 US Code § 2523 <https://www.govinfo.gov/content/pkg/USCODE-2019-title18/pdf/USCODE-2019-title18-partI-chap119-sec2523.pdf>.

731 Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L 119., art 1 and art 4.

732 EU Law Enforcement Directive, art 14-18.

733 Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 Eur Data Prot L Rev 367.

Box 8.2 – The impact of data localisation on data transfers

Data localisation has emerged as a key priority for several national jurisdictions with over 62 countries considering substantive legislation or planning upcoming policies.⁷³⁴ It essentially involves the development of regulations or policies that obliges data controllers to physically store personal data within the territorial boundaries of that country. Data localisation restricts the transfer of data to third countries and these restrictions can be unconditional or conditional. Unconditional restriction means that there is a restriction in terms of the transfer of all data outside the country irrespective of the sector. This can be seen in China and Russia, where no data can be transferred outside the country.⁷³⁵ While conditional restrictions limit the transfer of data based on the level of data protection in the third country, there can also be restrictions on data transfers in some sectors. For instance, personal electronic health sector data, in Australia, cannot be held or transferred to other countries.⁷³⁶ Other countries (such as Vietnam) ensure that all forms of their citizen's personal data are stored locally. Turkey has introduced an unconditional restriction on the financial sector to not transfer payments' data.⁷³⁷

734 Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (Information Technology and Innovation Foundation, 19 July 2021) page 18 <https://www2.itif.org/2021-data-localization.pdf>.

735 Scott Livingston, Graham Greenleaf, 'Data Localisation in China and Other APEC Jurisdictions' (2016) 143 *Privacy Laws and Business International Report*, 22-26 [2017] UNSWLRS 11 <http://www5.austlii.edu.au/au/journals/UNSWLRS/2017/11.pdf>.

736 Personally Controlled Electronic Health Record Act 2012, s 77

737 Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla. 'The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India' (2019) *The Centre for Internet and Society, India* <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.

Countries that have advocated for stringent data localisation norms often cite factors associated with national security and citizen's protection as key regulatory objectives. It is argued, for instance, that local storage of personal data ensures better access for the purpose of domestic law enforcement.⁷³⁸ However, it has also been contended that strengthening and making more efficient MLATs and other international agreements (such as the Council of Europe's Convention on Cybercrime) will support law enforcement without hampering the nature of the internet.⁷³⁹

Many countries exhibit a preference for localisation norms owing to concerns regarding foreign surveillance.⁷⁴⁰ Concerns associated with protecting national security and preventing cybercrime and data breaches are also additional factors which have brought about specific localisation policies in several jurisdictions.⁷⁴¹

Some of the arguments cited in favour of data localisation, such as enhanced cybersecurity, have been refuted by scholars, experts and civil society.⁷⁴² There is a general concern that state policies on data localisation will significantly transform the nature of the internet and unfairly restrict cross border data flows, thereby hampering digital trade.⁷⁴³ Furthermore, the collection and storage of personal data within the country may, in fact, result in a scenario where consolidated data stores become an easy target for data security breaches or domestic surveillance.⁷⁴⁴ Lastly, strict data localisation norms would significantly increase compliance costs for data controllers.⁷⁴⁵

- 738 Han-Wei Liu, 'Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism' in Pasha L Hsieh and Bryan Mercurio, *ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms* (Cambridge University Press 2019)
- 739 Anupam Chander, Uyen P. Le, 'Data Nationalism' (2015) 64(3) *Emory Law Journal* <https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=elj>.
- 740 Jonah Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders' (2014) *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance* <http://dx.doi.org/10.2139/ssrn.2430275>.
- 741 Dennis Broeders, 'Aligning the international protection of 'the public core of the internet' with state sovereignty and national security' (2017) 2(3) *Journal of Cyber Policy* 366 <https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1403640>.
- 742 Daniel Castro, 'The False Promise of Data Nationalism' (2013) *Info Tech and Innovation Foundation* (December 2013) *The Information Technology and Innovation Foundation* http://www2.itif.org/2013-false-promise-data-nationalism.pdf?_ga=2.78495325.87137249.1616122463-1857304164.1613993804.
- 743 Neha Mishra, 'Data Localization Laws in a Digital World: Data Protection or Data Protectionism?' (2016) *The Public Sphere, NUS Centre for International Law Research Paper* 19/05, 142 <https://psj.lse.ac.uk/articles/45/galley/44/download/>.
- 744 Tatevik Sargsyan, 'Data localization and the role of infrastructure for surveillance, privacy, and security.' (2016) 10 <*International Journal of Communication* <https://ijoc.org/index.php/ijoc/article/viewFile/3854/1648>; Anupam Chander, Uyen P. Le, 'Breaking the Web: Data Localization vs. the Global Internet' (2014). *Emory Law Journal*, Forthcoming, *UC Davis Legal Studies Research Paper No. 378*, Page 32 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.
- 745 Dan Svantesson, 'Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines' (2020) *OECD Digital Economy Papers* 301/2020 <https://doi.org/10.1787/7fbaed62-en>.

Key Considerations

- ◇ Whether a state provides adequate levels of data protection is critical in determining whether it can engage in data flows. Various legal instruments provide for differing standards to assess adequacy criteria. It is vital, however, that such assessments be made by independent authorities in a manner that is transparent, consultative, and reasonable.
- ◇ In the absence of adequacy, there are obligations of data protection that may be placed on data controllers by necessitating certain safeguards. These may take the form of instruments, such as contractual clauses that contain protections for personal data or even certification mechanisms that place such protection commitments on data controllers.
- ◇ Sufficient flexibility within frameworks should be provided. However, these derogations should be narrowly crafted with adequate protections. This is in order to ensure fair use and to allow for suitable changes and allowances for context specific transfers by using derogations which include consent, contractual or public interest necessity.
- ◇ Frameworks should also include provisions for adequate and proportional penalties for non-compliance and for domestic enforcement measures in the law.
- ◇ A broader concern to take into consideration is that both geographical and organisational norms for cross-border data flows need to co-exist. For instance, an adequacy requirement between countries is a geographical standard. Meanwhile, accountability, as set out by the APEC Privacy framework and through instruments such as SCCs and BCR, constitutes more of an organisational approach that is context specific.
- ◇ It is also important that accountability measures of supervisory authorities/regulators, as well as data controllers, take into consideration the actions and practices of the receiving country/organisation. This means ensuring that once personal information has been collected by an organisation, they continue to be accountable, for instance, through contractual clauses or rules to protect that data even if it moves from one jurisdiction to another.



CHAPTER 9

**STRUCTURE OF
REGULATORY
AUTHORITIES,
OFFENCES AND
PENALTIES**

9.1 Introduction

Regulatory bodies play an important role in enforcing data protection laws and regulation. They are central to ensuring the implementation of data protection and security standards and penalising actions that harm data subjects.⁷⁴⁶ They are typically designed to act as independent governmental bodies,⁷⁴⁷ and are either set up expressly for data protection purposes, or are required to oversee and enforce data protection in addition to other existing responsibilities.⁷⁴⁸

They may have adjudicatory powers and can be tasked with a host of other obligations. These powers may include the effective implementation and enforcement of relevant legislation, protection of data subjects' rights, subordinate rulemaking, and advising the state or public bodies on regulatory frameworks and issues relating to data protection.⁷⁴⁹ Rulemaking powers can also be shared with the executive in some cases. The Commonwealth PPI

and Privacy Bills (Commonwealth Bills) and HIPCAR Privacy Framework, for instance, allow the relevant Minister (assigned responsibility for information/public administration) to develop regulations to enforce the frameworks and prescribe necessary measures, subject to approval by Parliament.⁷⁵⁰

⁷⁴⁶ E.g. Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspective* (1st edn, OUP 2014), 3-4.

⁷⁴⁷ However, independence in practice can be difficult to achieve. See Philip Schütz, 'Comparing formal independence of data protection authorities in selected EU Member States' (4th Biennial ECPR Standing Group for Regulatory Governance Conference, Karlsruhe, 2012).

⁷⁴⁸ States need not necessarily set up new regulatory bodies for this purpose. For e.g., the UK's Information Commissioner's Office, which is charged with implementing data protection regulation in addition to other functions, has been in existence since 1984. The Information Commissioner's Office deals with information rights and covers a wide range of legislation, such as those relating to data protection, freedom of information, electronic communications, etc. See 'History of the ICO' (ICO) <https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/> accessed 19 October 2021; see also 'Legislations we cover' (ICO) <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/>.

⁷⁴⁹ The GDPR, for instance, requires States to set up independent public authorities to monitor and supervise the application of data protection law and provides various investigative and corrective powers to the authorities. See 'What are Data Protection Authorities (DPAs) and how do I contact them?' (European Commission) https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/what-are-data-protection-authorities-dpas-and-how-do-i-contact-them_en; in contrast, the US does not have a specific federal data protection authority, but the Federal Trade Commission is authorised to enforce privacy regulations in specific areas. State attorney generals and sector-specific regulators can also issue and enforce some privacy legislation. See 'Protecting Consumer Privacy and Security' (Federal Trade Commission) <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security> accessed 19 October 2021.

⁷⁵⁰ Commonwealth Privacy Bill, Part V, s 38; Commonwealth PPI Bill, s 44; HIPCAR Model Legislative Text, s 80.



Each of the Identified Regional Frameworks provides a varying level of detail about the regulatory structure and the supervisory or enforcement authority in charge of implementing obligations under the frameworks (Regulator). This is because some frameworks provide states with more leeway than others to design the structure and define the roles of Regulators in their domestic contexts. The OECD Guidelines, the APEC Privacy Framework, and the OAS Principles, for instance, provide very limited guidance on the Regulator and regulatory structure (Please refer to Box 1). The ASEAN DP Framework, meanwhile, does not contain any details about the regulatory structure or the Regulator. The APEC Privacy Framework, however, applies to most ASEAN countries.⁷⁵¹

Frameworks that provide more detailed guidance on the regulatory structure and Regulator are the GDPR, Convention 108+, the AU Convention, the HIPCAR Privacy Framework, and the Commonwealth PPI and Privacy Bills (Specified Frameworks). Under the Commonwealth Bills, the Commonwealth Privacy Bill creates the office of the Privacy Commissioner, which is also applicable to the Commonwealth PPI Bill. For this reason, references to the Privacy Bill in this chapter will generally also include the PPI Bill unless otherwise indicated.

This chapter proceeds as follows:

- Effective Regulatory Design (section 9.2) – Independence, transparency and accountability, inter-sectoral coordination
- Structure of the Regulator (section 9.3)
 - a. Composition, appointment, and qualifications of the Regulator and its officers/members
 - b. Funding and resources
 - c. Immunity and confidentiality
- Functions and Powers of the Regulator (section 9.4)
- Penalties, remedies, and appeals (section 9.5)

⁷⁵¹ This would be a non-binding, voluntary commitment. See ‘ASEAN Member States’ (ASEAN) <https://asean.org/about-asean/member-states/>; see also ‘What is Asia-Pacific Economic Cooperation?’ (APEC) <https://www.apec.org/about-us/about-apec>.

Box 9.1: Data Protection Regional Frameworks with limited guidance

Of the Identified Frameworks, those that provide limited guidance usually do so with the understanding that detailed national implementation would vary based on different legal systems and traditions, and that states are able to formulate the most appropriate implementation mechanism based on their domestic legal systems. However, they also include some limited recommendations. For instance, the OECD Guidelines require states to establish enforcement authorities “with the governance, resources, and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial, and consistent basis,” and provide for adequate sanctions and remedies in case of non-compliance with laws protecting privacy. They also allow states to set up specific supervisory bodies or rely on existing facilities and bodies.⁷⁵²

Similarly, the APEC Privacy Framework specifies that it is intended to be implemented in a flexible manner which can include various methods, such as the involvement of central data protection authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of these systems. It highlights the importance of educating and informing data subjects and controllers about domestic privacy protections, of cooperation and dialogue between public and private sectors, and of considering private sector opinions in developing privacy protections. It states that privacy protections should include an array of remedies for violations based on the domestic legal system and the extent of potential harm due to the violations. States must also periodically provide information to the APEC about relevant updates with regards to the domestic framework’s implementation in the state.⁷⁵³

752 OECD Guidelines, Chapter 1, Part 5, paras 19(c) and 19(f), p 62.

753 APEC Privacy Framework, Part iv, para 37, Part v, para 48, Part vi, Part vii, and Part viii, para 55.

The OAS Principles require that its Member States establish “independent and sufficiently funded supervisory bodies” to monitor and promote personal data protection.⁷⁵⁴ They also require Member States to provide the resources, funding, and technical expertise necessary for the authorities to effectively perform their duties.⁷⁵⁵

The OAS Principles note that the authorities can be set up at the national, regional, or municipal levels based on a country’s domestic legal and administrative structure. They specify that there is no uniform implementation approach in the region.⁷⁵⁶ Interestingly, the Principles also state that the authorities’ regulatory mandates may differ and that responsibility may be shared between regulatory bodies and private entities that are required to comply with specific obligations.

They also require that domestic law provides supervisory authorities with the ability to cooperate with each other, as well as with other relevant domestic stakeholders. Member States are also required to create reasonable means for data subjects to exercise their rights, encourage and support self-regulation for controllers and processors, and provide for adequate sanctions and remedies to protect the rights of data subjects and penalise noncompliance.⁷⁵⁷

754 OAS Principles with Annotations, Principle 13, p 27.

755 OAS Principles with Annotations, Principle 13, p 27.

756 OAS Principles with Annotations, “Data Protection Authority”, p 6, and Principle 13, p 27.

757 OAS Principles with Annotations, Principle 13, p 27.

9.2 Effective Regulatory Design

There are multiple factors that contribute to the creation of a robust regulator. Some depend on the regulation's subject matter (such as having clarity on the role of the regulator, regulatory objectives, and functions) and on domestic legal and administrative frameworks. The effective implementation of regulatory goals also generally depends on regulatory independence, transparency, and accountability - and especially in the context of data protection, inter-sectoral coordination. These are briefly introduced below and explored in more detail through the rest of this chapter.

9.2.1 Independence

Regulatory independence from the executive is a critical factor in the effectiveness of the data protection regime, since the state is one of the largest collectors and processors of personal data. Establishing an independent regulator can provide greater confidence for those that are regulated, and, for data subjects, that decisions are made fairly. An independent regulator is especially important in cases when both government and non-government bodies are subject to the same framework.⁷⁵⁸ Although providing for independence through legislation is not sufficient to guarantee independence, it is an important first step.⁷⁵⁹

The Specified Frameworks all recognise the importance of regulatory independence. The GDPR, Convention 108+, AU Convention, and the HIPCAR Privacy Framework specifically require that Regulators function independently and prohibit them from taking external instructions.⁷⁶⁰ While it does not include a separate provision for this, the Commonwealth Privacy

Bill notes the importance of ensuring independence when providing for a Commissioner.⁷⁶¹

Several elements can contribute to ensuring the regulator's independence, such as the composition of members, the process and manner of appointments and dismissal, the process for establishing whether there are conflicts of interest, adequate and transparent funding, and immunity from legal action, many of which have been covered by the frameworks. Independent operation, funding and resource allocation and immunity from legal actions are elements that most of the Specified Frameworks include provisions for.

9.2.2 Transparency and accountability

A lack of oversight mechanisms over the regulator may make it easier for them to exercise their powers in arbitrary ways, misuse funds, undertake cursory investigations and ignore due process requirements.⁷⁶² Consequently, independence of the regulator should ideally be combined with effective accountability mechanisms for the regulator to comply with to guard against abuse. Some of these measures can include regulatory reviews and reporting requirements. The GDPR specifically states that the independence of the supervisory authorities does not mean that they are exempt from control or monitoring mechanisms in relation to their financial expenditures or judicial review.⁷⁶³ Additionally, as per the GDPR, the exercise of the regulator's powers are subject to appropriate safeguards as set out in domestic law.⁷⁶⁴

⁷⁵⁸ OECD Guidelines, p 47-48.

⁷⁵⁹ Mark Thatcher, 'Regulation after delegation: independent regulatory agencies in Europe' (2002) *Journal of European Public Policy* 954; Fabrizio Gilardi and Martino Maggetti, 'The Independence of Regulatory Authorities' in David Levi-Faur (ed), *The Handbook on The Politics of Regulation* (Elgar Publishing, 2013)

⁷⁶⁰ GDPR, arts 52(1) and 52(2); Convention 108+, art 15(5); AU Convention, art 11(7); HIPCAR Model Legislative Text, s 54.

⁷⁶¹ Commonwealth Privacy Bill, p 3.

⁷⁶² Christel Koop and Chris Hanretty, 'Political Independence, Accountability, and the Quality of Regulatory Decision-Making' (2018) 51 *Comparative Political Studies* 38, p 9-10.

⁷⁶³ GDPR, recital 118.

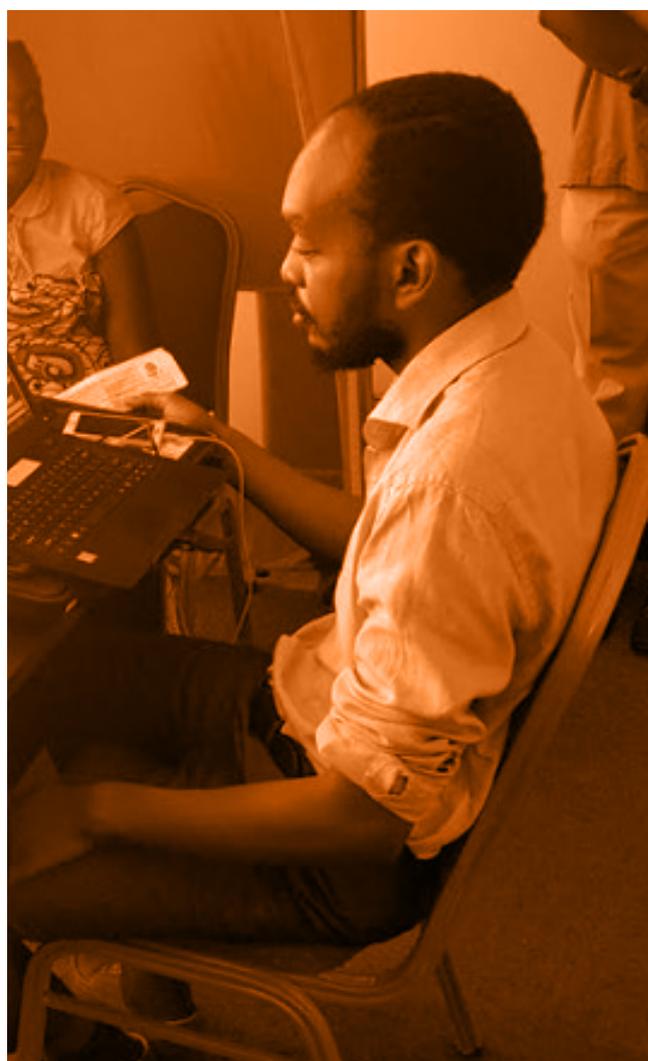
⁷⁶⁴ GDPR, art 58(4).

Reporting requirements are the most common method used to promote transparency and accountability of the Regulator in the Specified Frameworks. Reporting can increase credibility of the Regulator and detect early signs of emerging vulnerabilities.⁷⁶⁵ Nevertheless, research suggests that unless it is tailored to specific contexts, some reporting measures, such as the requirements to produce annual plans and reports could lead to increased costs, workloads, and bureaucracy without necessarily improving the regulator's functioning.⁷⁶⁶

Similarly, it is also important to design for the regulator's accountability to multiple stakeholders, such as to the legislature, regulated entities and to the larger public.⁷⁶⁷ An oversight body such as a management board that offers diverse expertise and transparency could also be beneficial in this regard.⁷⁶⁸ The regulator would be responsible for regulatory decision-making, and the oversight body would be responsible for oversight, scrutiny, and guidance of the regulator's operations.

9.2.3 Inter-sectoral coordination

Inter-sectoral coordination is especially important in the context of data protection because of the wide range of applications of personal data that range from healthcare to finance to public service delivery. Mandating cooperation mechanisms and engagement in regulation-making, especially through tools such as Memoranda of Understanding, can be particularly useful in this context.⁷⁶⁹



765 Malavika Raghavan, Beni Chugh and Nishanth Kumar, 'Effective Enforcement of a Data Protection: A Model for Risk-Based Supervision Using Responsive Regulatory Tools', 18 (Dvara Research, 1 November 2019) <https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>.

766 Christel Koop and Chris Hanretty, 'Political Independence, Accountability, And The Quality Of Regulatory Decision-Making' (2018) 51 *Comparative Political Studies*.

767 See 'OECD best practices for regulatory policy' ch 4 (OECD iLibrary) https://read.oecd-ilibrary.org/governance/the-governance-of-regulators/chapter-4-accountability-and-transparency_9789264209015-9-en#page1.

768 Malavika Raghavan, Beni Chugh and Nishanth Kumar, 'Effective Enforcement of a Data Protection: A Model for Risk-Based Supervision Using Responsive Regulatory Tools', 17-18 (Dvara Research, 1 November 2019) <https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>.

769 Dvara Research, 'Comments to the Ministry of Electronics and Information Technology (MeitY) on the draft Personal Data Protection Bill 2018, dated 27 July 2018, submitted by the Committee of Experts on a Data Protection Framework for India', 67 (Dvara Research, 2018) https://www.dvara.com/blog/wp-content/uploads/2018/10/Response-to-draft-Personal-Data-Protection-Bill_DvaraResearch.pdf; see also Malavika Raghavan, Beni Chugh and Nishanth Kumar, 'Effective Enforcement of a Data Protection: A Model for Risk-Based Supervision Using Responsive Regulatory Tools', 17-18 (Dvara Research, 1 Nov 2019) <https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>.

9.3 Structure of the Regulator

Box 9.2: Data protection regulatory models

Different jurisdictions have adopted various regulatory models for data protection. Some states have a more traditional regulator similar to what is found in the GDPR, in terms of a public authority specifically tasked with monitoring and enforcing the relevant data protection legislation. This type of model exists in countries such as Ireland, South Africa and in India's proposed data protection legislation.⁷⁷⁰ Some countries have regulators who oversee data protection and related matters, such as access to information. For instance, South Africa's Information Regulator is tasked with functions under both the Protection of Personal Information Act, and the Promotion of Access to Information Act.⁷⁷¹ Australia's Information Commissioner similarly has functions relating to privacy, freedom of information, and government information policy.⁷⁷²

770 'Who are we?' (Data Protection Commission) <https://www.dataprotection.ie/en/who-we-are>; Protection of Personal Information Act, 2019, s 39 <https://popia.co.za/section-39-establishment-of-information-regulator/>; The Personal Data Protection Bill, 2019 (India) http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. See also, Report of the Joint Committee on the Personal Data Protection Bill, 2019 available at https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.

771 The Protection of Personal Information Act, 2013, s 39 (South Africa) <https://www.justice.gov.za/inforeg/about.html>.

772 'About us' (OAIC) <https://www.oaic.gov.au/about-us/>; 'What we do' (OAIC) <https://www.oaic.gov.au/about-us/what-we-do/>.

An ombudsperson model is also one that has been explored. An ombudsperson is usually a public official appointed by the government and operates independently. For example, the Commonwealth PPI Bill makes it possible for the Privacy Commissioner recommended in the framework to be replaced by an alternate official, such as an ombudsperson.⁷⁷³ Finland's supervisory authority is the Data Protection Ombudsman, who is an autonomous and independent authority appointed by the government.⁷⁷⁴ The Data Protection Ombudsman and deputy ombudsmen form the Sanctions Board which is responsible for imposing administrative penalties. The Expert Board is an independent body of experts operating in connection with the Ombudsman and is tasked with issuing statements on significant data protection questions.⁷⁷⁵

Another model consists of mandating existing regulators with data protection obligations. This type of system is intended for countries where there is no state-level data protection legislation or specific regulator. This is the case in the United States. It has several sector and state-specific data protection laws offering varying levels of protection, but it does not have a single national-level data protection authority. However, the Federal Trade Commission uses its jurisdiction over commercial entities to protect consumers' personal information, especially in the context of unfair and deceptive trade practices.⁷⁷⁶ State Attorneys General usually have similar enforcement authority under consumer protection laws to prevent unfair and deceptive business practices.⁷⁷⁷

773 Summary of provisions of the Commonwealth PPI Bill, p 3.

774 Finnish Data Protection Act; 'Office of the Data Protection Ombudsman', s 8 <https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>.

775 Finnish Data Protection Act; 'Office of the Data Protection Ombudsman', s 12 and s 24 <https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>.

776 'Protecting Consumer Privacy and Security' (Federal Trade Commission) <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security>; 'Privacy and Security Enforcement' (Federal Trade Commission) <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>.

777 See for eg Carolyn Carter, 'Consumer Protection in the States – a 50-State report on unfair and deceptive Acts and Practices Statutes', 16 (National Consumer Law Center Inc February 2009) https://www.nclc.org/images/pdf/udap/report_50_states.pdf.

The composition, qualifications, and appointment processes implicate the independence of the Regulators and are important to the overall functioning and enforcement of the frameworks. They form part of the indicators that are used to assess the formal independence of regulators, which traditionally examine whether the independence of regulators is stated in law, and also evaluate the regulator's financial and organisational independence, and the functions that have been delegated to it.⁷⁷⁸ Formal independence assessments are related to, but may be different from, *de facto* independence, which relates to the extent of effective autonomy the regulator can utilise in practice. This would depend on a variety of factors such as the rule of law, the perceived legitimacy of regulatory bodies, and the political climate.⁷⁷⁹

9.3.1 Composition

The Specified Frameworks give states varying levels of discretion in determining the Regulator's structure so that a model is found that works best in a particular domestic scenario. Having an independent regulatory body specialising in data protection can be helpful since both governmental and non-governmental entities are regulated under the same framework.⁷⁸⁰ The AU Convention does not prescribe any conditions for the composition of the National Protection Authorities and only requires that states establish an administrative authority in charge of protecting personal data.⁷⁸¹ In comparison, the Commonwealth Privacy Bill creates the office of the Privacy Commissioner with specified powers and

functions, but includes it only on an optional basis which allows states to designate an existing officer to perform functions relating to data protection.⁷⁸²

Other instruments discuss other aspects of the form and number of regulatory bodies. Convention 108+ and HIPCAR Privacy Framework, for instance, note that the relevant Regulator may consist of a single commissioner or collegiate or other body, as long as it has certain powers and is able to effectively discharge its duties.⁷⁸³ The GDPR and Convention 108+ allow for the establishment of one or more independent public supervisory authorities to oversee their implementation.⁷⁸⁴ Convention 108+ states that it may also be useful to institute authorities whose ambit is limited to data protection in specific sectors, such as health, electronic communication, etc.⁷⁸⁵ Having a multi-member regulatory body can serve to increase independence since multiple members are less likely to be susceptible to influence than a single decision-maker, and can increase diversity and bring multiple perspectives and varied experience to the decision-making process.⁷⁸⁶

778 Fabrizio Gilardi and Martino Maggetti, 'The independence of regulatory authorities' in David Levi-Faur (ed), *The Handbook on The Politics of Regulation* (Edward Elgar Publishing 2013), pp 202 -203.

779 Fabrizio Gilardi and Martino Maggetti, 'The independence of regulatory authorities' in David Levi-Faur (ed), *The Handbook on The Politics Of Regulation* (Edward Elgar Publishing 2013), p 204; Chris Hanretty and Christel Koop, 'Shall the Law Set Them Free? The Formal and Actual Independence of Regulatory Agencies' (2013) 7 *Regulation and Governance*, pp 195, 197-199.

780 'The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy' (OECD iLibrary) 49 https://www.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en.

781 AU Convention, arts 11(1) and 11(3).

782 Commonwealth Privacy Bill, Part, p 3, which allows States that may not be able to create a separate office for this purpose to designate an existing officer to perform critical functions relating to privacy protection. It specifies that the officer must have adequate independence, and that the functioning of the framework would not be jeopardised.

783 Explanatory Report to the Convention 108+, paras 117 and 119, p 28-29; HIPCAR Model Legislative Text, ss 48(1),48(3), 39 and Explanatory Notes to HIPCAR Model Legislative Text, para 68.

784 GDPR, art 51(1), recital 117; Convention 108+ art 15(1), Explanatory Report to the Convention 108+, para 118, p 30; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows art 1(1); 'Treaty office' (Council of Europe Portal) <https://rm.coe.int/1680080626>.

785 Convention 108+, art 15(1), Explanatory Report to the Convention 108+, para 118, p 29.

786 'The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy' (OECD iLibrary) 70-71 https://www.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en.

Unlike other frameworks, the European Union also has a cross-national body to oversee data protection. The European Data Protection Board (EDPB), set up under the GDPR and comprising representatives of the EU national data protection authorities, is an independent body responsible for ensuring the GDPR's consistent application throughout the EU. It is tasked with providing general guidance on data protection laws, advising the European Commission and national supervisory authorities, settling disputes between national supervisory authorities, as well as promoting cooperation between the authorities.⁷⁸⁷

9.3.2 Appointment

Having a transparent appointment processes for the Regulator's members can play an important role in increasing both actual and perceived independence, and has become one of the most frequently used metrics to assess formal independence.⁷⁸⁸

The GDPR, HIPCAR Privacy Framework, and Commonwealth Privacy Bill provide for some appointment procedures while the AU Convention and Convention 108+ leave it to the discretion of relevant states.

The GDPR requires supervisory authorities to be appointed by a transparent procedure which involves the parliament, government, head of state, or an independent body entrusted with making the appointment according to the law. States must also have laws that provide for the establishment of the supervisory authority, and which must include details relating to the engagement of its members.⁷⁸⁹ This can encourage formal independence and increase transparency and accountability.

Although the HIPCAR Privacy Framework does not contain much detail, it specifies that the Data Commissioner must be appointed by a country's

head of state, in consultation with the Prime Minister and the Leader of the Opposition.⁷⁹⁰ It is not clear whether consultation means agreement and how any disagreements are to be addressed. Similarly, the Commonwealth Privacy Bill provides that the Privacy Commissioner must be appointed by the President or other head of state on the recommendation of the Minister,⁷⁹¹ and must be subject to the terms specified in the instrument of appointment.⁷⁹²

9.3.3 Qualifications, disqualifications, tenure, removal/dismissal, and confidentiality

9.3.3.1 Qualifications

Requiring prior experience or expertise in data protection and related areas could equip the Regulator with the necessary tools to effectively perform its duties. The GDPR sets out broad qualifications for members of supervisory authorities, requiring them to have the qualifications, experience, and skills, particularly in personal data protection to perform their duties and functions. It also requires states to provide by law specific qualifications and eligibility criteria for members' appointment.⁷⁹³ The other Specified Frameworks do not provide qualifications or eligibility criteria, but detail disqualifications for the relevant Regulators.⁷⁹⁴

9.3.3.2 Disqualifications

Disqualifications from membership from regulatory bodies are usually meant to prevent conflicts of interest and undue influence. The GDPR does not specify disqualifications but requires members of supervisory authorities to refrain from actions incompatible with their duties and from engaging in "incompatible occupations" during their term of office.⁷⁹⁵ The requirement to not engage in other

787 See GDPR recital 72, arts 40-42, and Chapter VII on cooperation and consistency. See also 'Who are we' (European Data Protection Board) https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en.

788 OECD, Being an Independent Regulator (OECD Publishing 2016) 38-42.

789 GDPR, arts 53(1) and 54(1).

790 HIPCAR Model Legislative Text, s 48.

791 Commonwealth Privacy Bill, Part I, s 4 specifies that "'Minister" means the Minister who has been assigned responsibility for [information/public administration] under the Constitution."

792 Commonwealth Privacy Bill, Part III, ss 16 and 20.

793 GDPR, arts 53(2) and 54(1)(b).

794 HIPCAR Model Legislative Text, s 48; Commonwealth Privacy Bill, Part III, s 18; AU Convention, art 11(6).

795 GDPR, arts 54(1)(b) and 52(3).

occupations during their mandate is also reflected in the HIPCAR Privacy Framework and the AU Convention.⁷⁹⁶

The HIPCAR Privacy Framework, the Commonwealth Privacy Bill and the AU Convention also contain more specific disqualifications, such as membership in the executive or judiciary, bankruptcy, or conviction of certain offences involving dishonesty or moral turpitude.⁷⁹⁷ The AU Convention additionally bars those engaged as business executives or owning shares in businesses in the information and communication technologies sector.⁷⁹⁸ The Commonwealth Privacy Bill requires the Privacy Commissioner to be a full-time official who cannot be employed in any other capacity during their term of office. They are also thereafter ineligible for appointment in public service.⁷⁹⁹

9.3.3.3 Term

Requiring fixed terms for the Regulator's members, specified in law, can prevent arbitrary dismissals and reappointments and serve to maintain independence. The HIPCAR Privacy Framework and Commonwealth Privacy Bill specify that the term of appointment for the Commissioner should be for five years and that Commissioners are eligible for reappointment at the end of their term.⁸⁰⁰ The GDPR sets a minimum term of four years and leaves the determination of reappointment to states.⁸⁰¹ Convention 108+ and the AU Convention do not discuss the length of term appointments of the Regulator or of its members.

9.3.3.4 Dismissal/removal/vacancy

Explicit removal and dismissal procedures that are limited to serious misbehaviour and involve non-executive arms of government, such as the legislature or judiciary, is critical for greater transparency and accountability.⁸⁰² The GDPR, HIPCAR Privacy Framework, and Commonwealth Privacy Bill specify that members can only be dismissed for just cause, such as when there is serious misconduct or if they no longer fulfil the conditions required to perform their duties.⁸⁰³ The HIPCAR Privacy Framework also allows the executive to appoint a temporary commissioner in certain circumstances, provided the existing Commissioner, who is being replaced, makes a written request to the effect that it is necessary that a temporary commissioner be appointed.⁸⁰⁴ Meanwhile, Convention 108+ and AU Convention do not discuss the removal or dismissal of the Regulator.

9.3.3.5 Funding and resources

Having adequate funding can significantly impact regulatory functioning and independence, and is key to attracting and retaining competent, qualified members. In addition to the source of funding, autonomy in managing funds is integral to the regulator being able to carry out its mandate and act independently.⁸⁰⁵ This includes being able to appoint its own staff. For example, the ECJ found supervisory authorities to be not completely independent when the staff was supplied by the state and the state had to be informed of the work undertaken by the authority at all times.⁸⁰⁶

796 HIPCAR Model Legislative Text, s. 48; AU Convention, art 11(6).

797 HIPCAR Model Legislative Text, s 48; Commonwealth Privacy Bill, Part III, s. 18; AU Convention art 11(6).

798 AU Convention, art 11(6).

799 Commonwealth Privacy Bill, Part III, s 19.

800 HIPCAR Model Legislative Text, s 50(1); Commonwealth Privacy Bill, Part III, s17(1).

801 GDPR art 54(d), 54(e).

802 The OECD Guidelines, 29.

803 GDPR art 53(4); HIPCAR Model Legislative Text, s 50(3); Commonwealth Privacy Bill, Part III, ss 17 and 18(2).

804 See HIPCAR Model Legislative Text, s 48(5,6).

805 'The Governance of Regulators, Being an Independent Regulator' (OECD iLibrary) 71 https://read.oecd-ilibrary.org/governance/being-an-independent-regulator_9789264255401-en; 'The Governance of Regulators, Creating a Culture of Independence, Practical Guidance against Undue Influence' (OECD iLibrary) 14-15 https://read.oecd-ilibrary.org/governance/creating-a-culture-of-independence_9789264274198-en.

806 C-614/10 European Commission v Republic of Austria [2012] OJ L281/31. In this case, the Federal Chancellery of Austria supplied the supervisory authority with its workforce and the latter was required to inform the former about its work at all times. The ECJ found the supervisory authority to not be completely independent.

“All the Specified Frameworks require that states provide the necessary resources and funding for the Regulators to effectively perform their duties and to be able to appoint their own staff without interference.”

All the Specified Frameworks require that states provide the necessary resources and funding for the Regulators to effectively perform their duties and to be able to appoint their own staff without interference.⁸⁰⁷ The GDPR and HIPCAR Privacy Framework also highlight that the staff must be under the Regulator’s control.⁸⁰⁸ The GDPR, HIPCAR Privacy Framework, and Commonwealth Privacy Bill provide requirements regarding the sources of funding for the activities of the Regulators (for example, by having separate public annual budgets for the regulators) to enable them to function independently despite the fact that they are generally financed by the state.⁸⁰⁹

9.3.3.6 Immunity and confidentiality

The Commonwealth Privacy Bill, HIPCAR Privacy Framework, and AU Convention provide immunity to the Regulator and its staff from legal liability for actions undertaken in good faith and in the performance of their duties or exercise of their powers.⁸¹⁰ This is generally intended to maintain the independence of the Regulator. All Specified Frameworks also include some form of confidentiality requirement for Regulators.⁸¹¹ The GDPR, Convention 108+, and Commonwealth Bills specify that they apply to the Regulator, as well as to any staff and officers and are applicable during the term of engagement and thereafter.

807 Convention 108+ art 15(6); AU Convention art 11(8); Commonwealth Privacy Bill, Part III, s 22.

808 GDPR, arts 52(4) and 52(5); HIPCAR Model Legislative Text, s 48(3).

809 HIPCAR Model Legislative Text, s 51. The explanatory text to s 51 (in para 75) details the intention behind the provision; GDPR art 52(6), recital 120, Commonwealth Privacy Bill, Part III, s 22.

810 HIPCAR Model Legislative Text, s 52 and Explanatory Notes, para 76; Commonwealth Privacy Bill, Part IV, s 34, Commonwealth PPI Bill, s 41; AU Convention, art 11(7)(a).

811 AU Convention, art 11(5)(a); HIPCAR Model Legislative Text, s 56(1), 56(2); Commonwealth Privacy Bill, Part, Part IV ss 32 and 33; Commonwealth PPI Bill, ss 39 and 40; GDPR art 54(2); Convention 108+ art 15(8).

9.4 Functions and Powers of the Regulator

The Regulator is usually tasked with a wide range of responsibilities, such as monitoring and enforcing relevant legislation, providing information to data subjects, handling complaints, conducting investigations, authorising certain forms of processing, accrediting bodies and/or approving contractual clauses or monitoring arrangements, as well as maintaining relevant records. Regulators are given an array of powers that enable them to fulfil their assigned responsibilities. The Regulator's duties and powers can be explained as follows:

9.4.1 Monitoring and prior authorisation

Regulators are usually required to monitor and enforce relevant data protection legislation,⁸¹² and can also be required to monitor developments that have an impact on the protection of personal data.⁸¹³ This can help identify potential violations and support the initiation of pro-active enforcement actions. The AU Convention requires the National Protection Authority to ensure that information and communication technologies do not constitute a threat to public freedoms and the private life of citizens.⁸¹⁴

The AU Convention also requires controllers to declare data processing activities to the Regulator, and obtain prior authorisation for some certain kinds of processing activities. Other than for specifically exempted data processing categories and processing activities which are unlikely to constitute a breach

of privacy, personal data processing is subject to controllers declaring their processing activities before the National Protection Authority.⁸¹⁵ Some categories of data processing, such as those relating to genetic information and health, biometric data, data involving the national identity number or any other identifier, would require prior authorisation from the authority before processing.⁸¹⁶

The GDPR requires prior authorisation by law to undertake certain kinds of data processing. In such cases, supervisory authorities may consult with controllers and authorise processing for a task carried out in the public interest, for example when it relates to social protection or public health.⁸¹⁷

9.4.2 Complaints, investigations, and enforcement

Investigating violations and enforcing compliance are some of the Regulators' core functions and they are key to protecting the rights of data subjects. All Specified Frameworks require Regulators to handle complaints by data subjects or organisations and inform them of the investigations' progress or outcomes.⁸¹⁸ They are also required to play a proactive role in investigations. The HIPCAR Privacy Framework requires Data Commissioners to "exercise control on all data processing activities", either of their own accord or at the request of a data subject, and to verify whether it is carried out in accordance with the framework.⁸¹⁹ According to the Commonwealth

812 HIPCAR Model Legislative Text, ss 55(a) and 55(l); Commonwealth Privacy Bill, Part III, s 21(a); GDPR, art 57(1)(a); AU Convention 11(1)(b); Commonwealth Privacy Bill, Part II, s 21(a) (also applicable to Commonwealth PPI Bill, s 32(2)).

813 HIPCAR Model Legislative Text, s 55(n); GDPR 57(1)(i). The GDPR specifically mentions the development of information and communication technologies and commercial practices in this context, and HIPCAR-CARICOM the data processing and information technology. See GDPR 57(1)(i); HIPCAR Model Legislative Text, s 55(n).

814 AU Convention, art 12(2).

815 AU Convention, arts 10(2) and 10 (3). For exemptions, see art 9(2), art 10(1), art 10(4), and art 10(5).

816 AU Convention, art 10(4).

817 GDPR art 58(3)(c).

818 Convention 108+ art 15(4); AU Convention, art 12(2)(a) and 12(2)(e); HIPCAR Model Legislative Text, s 55(e); Commonwealth Privacy Bill, Part II, ss 21(c) and 21(g); GDPR 57(1)(f). The GDPR also requires data subjects to be informed of whether further investigation of coordination with another supervisory authority is required.

819 HIPCAR Model Legislative Text, s 55(c), (d).

Bills, Privacy Commissioners must inquire into any matters or developments if the privacy of individuals is being, or is likely to be, infringed upon.⁸²⁰ The GDPR also requires supervisory authorities to conduct investigations with regards to the GDPR's application, including on the basis of information received by another supervisory authority or public authority.⁸²¹

In a somewhat related and unique provision, the AU Convention requires National Protection Authorities to “speedily [inform] judicial authorities of certain types of offences that have come to their attention”, but it is unclear what these offences would involve.⁸²²

9.4.2.1 Complaints and investigations

The AU Convention, Convention 108+, and the HIPCAR Privacy Framework contain broad provisions providing Regulators with general powers of investigation and enforcement, such as “entertaining claims, petitions and complaints regarding the processing of personal data and informing the authors of the results thereof,” “powers of investigation and intervention”, or the power to undertake all activities that are necessary or connected to carrying out their duties.⁸²³

The Commonwealth Bills provide differing rights in respect to public authorities and private organisations. For public authorities, Privacy Commissioners are required to receive and investigate complaints regarding the collection, retention, or disposal of personal information and the use or disclosure of personal information.⁸²⁴ For private organisations, Privacy Commissioners must additionally receive and investigate complaints regarding the refusal of an organisation to grant access to information to data subjects, and the refusal of applications to correct their personal information.⁸²⁵ In both cases,

Commissioners must initiate a complaint when they believe that there are reasonable grounds to investigate.⁸²⁶ However, for data subjects, not being able to approach Commissioners to investigate public bodies' access refusals or applications to correct information can significantly impair their rights. As discussed in Chapter 5 (Rights of Data Subjects), the rights to access and rectification are foundational rights and the inability of individuals to exercise these rights against public authorities can impact the delivery of public benefits and services.

Frameworks also provide for Regulators to investigate specific reports of violations. This can be either upon receipt of a complaint or at the Regulators' own initiative.⁸²⁷ The HIPCAR Privacy Framework requires the Commissioner to investigate complaints unless it is of the opinion that it is frivolous or vexatious. The Commissioner must also notify data subjects of decisions with regards to their complaints and of their right to appeal.⁸²⁸ The HIPCAR Privacy Framework and the Commonwealth Bills also specify that Commissioners must notify the relevant processor or controller of their intention to investigate data processing undertaken by them, and of the substance of the complaint, before commencing the investigation.⁸²⁹ In this context, the GDPR, Convention 108+, and AU Convention require Regulators to cooperate and coordinate with other regulators to ensure the consistent application of the relevant framework.⁸³⁰ Regulators also have other investigative powers which are explored below.

820 Commonwealth Privacy Bill, Part II, s 21(d). See also Commonwealth PPI Bill, s 32(2).

821 GDPR, art 57(1)(h).

822 AU Convention, art 12(2)(f).

823 AU Convention, art 12(2)(e); Convention 108+, art 15(2)(a); Explanatory Report to the Convention 108+, para 120, p 29; HIPCAR Model Legislative Text, s 57.

824 Commonwealth Privacy Bill, Part IV, s 23(1).

825 Commonwealth PPI Bill, s 29(1).

826 Commonwealth Privacy Bill, Part IV, s 23(3); Commonwealth PPI Bill, 29(3).

827 See Commonwealth Privacy Bill, Part IV, s 23; Commonwealth PPI Bill, s 29. With private bodies, they can additionally investigate refusals to grant access to or correct personal information. See also Commonwealth PPI Bill, ss 29(1)(c) and 29(1)(d); HIPCAR Model Legislative Text, s 62(1).

828 HIPCAR Model Legislative Text, s 62(2).

829 HIPCAR Model Legislative Text, s 64; Commonwealth Privacy Bill, Part IV, s 25; Commonwealth PPI Bill, s 31.

830 GDPR, art 57(1)(g); AU Convention, arts 12(1) and 12(2)(m); HIPCAR Model Legislative Text, s 55(k); Convention 108+, arts 16,17,22, and ch VI.

Audits

The GDPR allows supervisory authorities to carry out investigations in the form of data protection audits and reviews of previously issued data protection certifications, and to also notify controllers and processors of alleged infringements of the framework.⁸³¹ Measures such as audits, impact assessments, and prior authorisations/consultations can serve to prevent violations of the framework and reduce the number of complaints and post-facto investigations.

The AU Convention states that the National Protection Authority is responsible for “undertaking the audit of all processed personal data, through its officials or sworn officials.”⁸³² It is unclear, however, what specifically the audits involve. The Commonwealth Bills contain a somewhat related provision allowing Privacy Commissioners to periodically carry out investigations with respect to personal information controlled by public or private entities.⁸³³ This is to ensure compliance with their obligations under the frameworks.

Access to information and procedural powers

Most Specified Frameworks provide Regulators with the power to obtain the necessary information to conduct their investigations. This is essential for regulators to be able to effectively investigate potential contraventions. The Commonwealth Bills provide quasi-judicial powers to Privacy Commissioners in carrying out investigations, ranging from summoning and enforcing the appearance of persons before them, to compelling or receiving evidence, to entering premises and obtaining copies and extracts of records. They allow Commissioners to determine the procedure to be followed in discharging any of their duties or performing any of their functions.⁸³⁴ Likewise, the AU Convention and Commonwealth Bills allow the relevant Regulators to determine the procedure to be followed in discharging their duties.⁸³⁵

“Most Specified Frameworks provide Regulators with the power to obtain the necessary information to conduct their investigations..”

831 GDPR, arts 58(1)(b), 58(1)(c), and 58(1)(d).

832 AU Convention, art 12(2)(g).

833 Commonwealth Privacy Bill, Part IV, s 30; Commonwealth PPI Bill, s 37.

834 Commonwealth Privacy Bill, Part IV, ss 26 and 28; Commonwealth PPI Bill, ss 32 and 34.

835 AU Convention, art 11(5)(b); Commonwealth Privacy Bill, Part IV, s 26; Commonwealth PPI Bill, s 32.

The GDPR and HIPCAR Privacy Framework provide specific powers to Regulators in the context of access to information and equipment for performing their functions. The GDPR allows supervisory authorities to order data controllers and data processors to provide any information and access to all information and personal data required to perform their tasks. Controllers and processors are also required to provide access to any premises and equipment in accordance with domestic law.⁸³⁶

Similarly, the HIPCAR Privacy Framework allows the Data Commissioner to require persons to provide access to personal data and related information.⁸³⁷ It also allows the Commissioner to delegate any of its investigative and enforcement powers to any authorised officer that it designates for that purpose.⁸³⁸

Where public authorities disclose personal information pursuant to the Commonwealth Privacy Bill, it specifies that an assertion that a disclosure was made in good faith constitutes an absolute response in civil or criminal proceedings against such public authorities.⁸³⁹ Although this is restricted only to information disclosure, the lack of accountability on such “good faith” actions could impair data subject rights.

Reporting requirements and confidentiality of investigation

Most Specified Frameworks provide that the Regulator works with judicial and other authorities to enforce the relevant framework. For example, the GDPR, Convention 108+, and AU Convention give Regulators the power to bring infringements to the

attention of judicial authorities and commence or engage in legal proceedings in order to enforce the framework.⁸⁴⁰ When an investigation reveals that an offence may have been committed under the framework, the HIPCAR Privacy Framework requires the Data Commissioner to refer the matter to the Police Commissioner for further action.⁸⁴¹

The HIPCAR Privacy Framework and Commonwealth Bills also specify that investigations of complaints under the framework must be conducted in private. Concerned parties must be provided with the opportunity to make representations to the Commissioner, but no one is entitled to be present when the representations are made, or to have access to or comment on representations made to the Commissioner by the other parties.⁸⁴²

9.4.3 Advising governments and other stakeholders, and approving codes of conduct

9.4.3.1 Advisory functions

Advising governments

Regulators are given advisory functions under each of the Specified Frameworks, and usually to improve or design legislative and administrative measures.⁸⁴³ This can involve requiring the government to consult the Regulator on proposals to introduce measures that relate to personal data processing, or providing opinions or information on general legislative or administrative measures, or other actions that might improve privacy protections.⁸⁴⁴ Convention 108+ and

836 GDPR, arts 58(1)(a), 58(1)(e), and 58(1)(f).

837 HIPCAR Model Legislative Text, s 58 (1), 58(2). The information is to be requested through a written information notice, which must specify (a) the time for compliance, which is to not be less than 30 days; and (b) that the person to whom the notice is addressed has the right of appeal within 30 days, see s 59. It also specifies that other laws restricting or prohibiting disclosure of information would not prevent persons from disclosing necessary information to the Commissioner, unless the information is necessary to safeguard national security or relates to privileged proceedings in Court, see s 58 (3), 58(4).

838 It does not specify who an ‘authorised officer’ would be or any guidelines for how police officers would be chosen, but notes that this power is provided to ensure operational and organizational practicality. HIPCAR Model Legislative Text, s 53.

839 Commonwealth Privacy Bill, Part V, s 37.

840 GDPR, art 58(5); Convention 108+, art 15(2)(d); AU Convention, art 12(2)(f). This is framed as a requirement under the AU.

841 HIPCAR Model Legislative Text, s 71.

842 HIPCAR Model Legislative Text, s 70, also see s 44 (commissioner may hold enquiries in private); Commonwealth Privacy Bill, Part IV, s 27, Commonwealth PPI Bill, s 33.

843 GDPR, art 57(1)(c); AU Convention, art 12(2)(l); HIPCAR Model Legislative Text, s 55(i); Commonwealth Privacy Bill, Part III, s 21(k) (and Commonwealth PPI Bill, s 32(2)).

844 Convention 108+, art 15(3); Commonwealth Privacy Bill, Part III, ss 21(k) and 21(l) (and Commonwealth PPI Bill, because of s 32(2)); HIPCAR Model Legislative Text, s 55(j); also see Commonwealth Privacy Bill, Part III, ss 21(h) and 21(i).

GDPR empower supervisory authorities to provide opinions to the national parliament, government, other institution or body, or the public, on any issue relating to personal data protection either on request or at their own initiative.⁸⁴⁵ These measures can serve as a means to ensure that data protection considerations are taken into account when framing regulations or measures in specific sectors and can encourage inter-sectoral cooperation.

The role of regulatory authorities has been highlighted during the COVID-19 pandemic. It has required the processing of different types of data, such as those related to health and location information. There has been ambiguity on the extent of permissible data processing. Many domestic regulators and the EDPB have issued guidance and advisories on related issues over the course of the pandemic and have provided some clarity to data subjects, controllers and other stakeholders as to how data protection legislation should apply in unforeseen circumstances.⁸⁴⁶

Advising controllers

Regulators can be required to guide and advise controllers to ensure that they comply with relevant data protection frameworks. For instance, the GDPR provides supervisory authorities with the power to advise controllers before they undertake processing in the case when a data protection impact assessment indicates a high risk to the data subjects' rights and freedoms.⁸⁴⁷ States can also require controllers to consult with, and obtain prior authorisation from, supervisory authorities in the performance of tasks in the public interest, such as relating to social

protection or public health.⁸⁴⁸

Under the AU Convention, the National Protection Authorities are required to advise those engaged in personal data processing or carrying out tests and experiments likely to result in data processing.⁸⁴⁹ The Commonwealth Bills contain a broader requirement for the Privacy Commissioner to provide advice on obligations and the framework's general operational mandate to public and private entities that process personal data.⁸⁵⁰ All Specified Frameworks also require Regulators to promote public awareness by informing data subjects of their rights under the relevant data protection laws.⁸⁵¹

9.4.3.2 Codes of conduct

The GDPR and HIPCAR Privacy Framework provide for the creation of codes of conduct meant to guide those processing personal data. This can provide clarity for processors and controllers and assist them in complying with data protection requirements.

The HIPCAR Privacy Framework provides for the creation of both mandatory and voluntary codes to promote the application of the privacy principles outlined in the framework.⁸⁵² The Commissioner is also required to guide their development, promote awareness, approve codes, and undertake related actions as necessary.⁸⁵³ Under the GDPR, supervisory authorities must encourage codes of conduct intended to contribute to the proper application of the framework, and account for specific features of various sectors and the needs of micro, small, and

845 GDPR, art 58(3)(b); Explanatory Report to the Convention 108+, para 126, p 30. The Explanatory Report specifies that only general measures are meant to be covered by this consultative power.

846 See eg 'Statement by the EDPB chair on data processing in the context of the COVID-19 outbreak' (EDPB) https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_hu; also see EDPB guidelines on the use of location data and contact tracing tools in the context of the COVID-19 pandemic: 'Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak' (EDPB) https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_hu; also see the UK Information Commissioner's Data Protection and Coronavirus Information Hub: 'Data protection and coronavirus information hub' (ICO.) <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/>; New Zealand's Privacy Commissioner's guidance on privacy and COVID-19: 'Privacy and COVID-19' (Privacy Commissioner) <https://www.privacy.org.nz/resources-2/privacy-and-covid-19/>.

847 GDPR, art 58(3)(a).

848 GDPR, art 36(3).

849 AU Convention, art 12(2)(j).

850 Commonwealth Privacy Bill, Part III, s 21(b); also applicable to private organizations under the Commonwealth PPI Bill, owing to s 32(2).

851 GDPR, art 57(1)(b) (see also recitals 13a1,132); AU Convention art 11(2), 12(2)(b); Convention 108+, art 15(2)(e)(ii); HIPCAR Model Legislative Text, ss 55(g) and 55(h); Commonwealth Privacy Bill, Part III, s 21(e) (also Commonwealth PPI Bill, because of s 32(2)).

852 HIPCAR Model Legislative Text, ss 20 and 21.

853 HIPCAR Model Legislative Text, s 55(m), see also s 21(1), 21(2).

medium-sized enterprises.⁸⁵⁴ Convention 108+ does not specifically provide for codes of conduct, but nevertheless notes that domestic law may be usefully reinforced by voluntary measures, such as codes of good practice or professional conduct.⁸⁵⁵

9.4.4 Impact assessments, certification and accreditation, and standard contractual clauses

Some Identified Regional Frameworks also provide for impact assessments, certification and accreditation mechanisms, and adoption of standard contractual clauses. For instance, as discussed in Chapter 4 (Transparency and Accountability), the GDPR, HIPCAR Privacy Framework, and Convention 108+ provide for impact assessments. The GDPR also has provisions on standard contractual clauses and binding corporate rules applicable in the context of data transfers to other countries as mentioned in Chapter 8 (Regulation of Cross-Border Data Flows). It also provides for certification and accreditation mechanisms which can be used to demonstrate compliance with the framework.⁸⁵⁶

9.4.5 Record-keeping, research, and reporting

Record-keeping and reporting requirements can increase transparency and provide a basis to assess regulatory performance. The GDPR requires supervisory authorities to keep records of framework violations and resultant corrective measures.⁸⁵⁷ Although only the GDPR contains this specific requirement, all the Specified Frameworks require Regulators to submit periodic activity reports to the national parliament, the general public, or other relevant authorities.⁸⁵⁸ The reporting details and the entities to which reports must be submitted vary across countries.⁸⁵⁹



The HIPCAR Privacy Framework and the Commonwealth Bills additionally contain research and reporting requirements.⁸⁶⁰ This can encourage the development of expertise, provide information on regulatory focus areas, and highlight important data protection issues. Research is generally to be undertaken in areas relating to information technology and data processing. The HIPCAR Privacy Framework requires that Regulators include results of research and monitoring on developments in data processing and information technology, if any, in their annual report to parliament.⁸⁶¹

The framework also requires Data Commissioners to publish at least annually an index of personal information held by public authorities. This publication should include a summary of specific activities,

854 GDPR, arts 40(1), 40(2), and 57(1)(m).

855 Explanatory Report to the Convention 108+, para 33, p 19.

856 GDPR, art 42(1). See also GDPR arts 42(2), 57(1)(n), 57(1)(p), 57(1)(q). See for reviewing certifications and accreditations, GDPR, arts 42(7), 57(1)(o); art 43.

857 GDPR, art 57(1)(u).

858 GDPR, art 59; Convention 108+ art 15(7); AU Convention, art 12(2)(o) HIPCAR Model Legislative Text, s 72; Commonwealth Privacy Bill, Part IV, s 31; Commonwealth PPI Bill, s 38.

859 GDPR, art 59; Convention 108+, art 15(7); AU Convention, art 12(2)(o); HIPCAR Model Legislative Text, s 72; Commonwealth Privacy Bill, s 31 and Commonwealth PPI Bill, s 38.

860 Commonwealth Privacy Bill, Part III, s 21(i), 21(j), 21(n); HIPCAR Model Legislative Text, s 55(n).

861 HIPCAR Model Legislative Text, s 55(n).



“Record-keeping and reporting requirements can increase transparency and provide a basis to assess regulatory performance.”

such as privacy impact assessments conducted by Ministries, information systems under their control and other related information.⁸⁶² This acts as a governmental transparency tool and can serve to increase accountability.

Interestingly, the HIPCAR Privacy Framework also requires that Data Commissioners create and maintain a register of data controllers.⁸⁶³ The AU Convention contains a similar requirement whereby the National Protection Authorities are responsible for updating a processed personal data directory that is accessible to the public.⁸⁶⁴ However, it does not specify the details that such a directory should contain.

9.4.6 Residuary functions

The GDPR, HIPCAR Privacy Framework, and Commonwealth Bills all have provisions that enable Regulators to perform other unspecified necessary functions. This is typically included to provide flexibility for Regulators in the context of evolving technological innovations and their impact on data protection.⁸⁶⁵

⁸⁶² HIPCAR Model Legislative Text, s 33.

⁸⁶³ HIPCAR Model Legislative Text, s 55(b).

⁸⁶⁴ AU Convention, art 12(2)(i).

⁸⁶⁵ GDPR, art 57(1)(v); Commonwealth Privacy Bill, Part III, ss 21(o) and 21(p); HIPCAR Model Legislative Text, s 55(p) and 55(q).

9.5 Penalties, remedies, and appeals

The enforcement mechanisms available to Regulators and the penalties that they are empowered to impose can significantly impact the level of compliance with the relevant regulatory framework. While there are multiple approaches to regulatory enforcement and the level of punitive actions that may be chosen,⁸⁶⁶ having a range of enforcement tools can equip regulators in ensuring effective enforcement. It is especially important for regulators to be able to hold the state and its agencies liable for violations in order to keep them accountable and to develop public trust in the regulator. Moreover, informal influence from the executive and other parties over regulatory bodies can be difficult to detect and make it extremely challenging to hold them liable for regulatory breaches. Designing for and ensuring the independence of the regulators, both structurally and by increasing transparency in decision-making and providing reasoned decisions, is therefore paramount to ensure that regulators can meaningfully sanction the state and other stakeholders when required.⁸⁶⁷

Publishing guides and manuals detailing the policies and procedures to be used in enforcement can also increase transparency and accountability for enforcement proceedings.⁸⁶⁸ In addition to providing information to the public on the processes and considerations involved in regulatory action, it can help create regulatory certainty and reduce deviation from best practices.⁸⁶⁹ In this context, the GDPR specifies that the powers of supervisory authorities must be subject to appropriate safeguards set

out by law, including judicial remedy and due process.⁸⁷⁰ It also states that the Regulator's legally binding measures must be in writing, be clear and unambiguous, provide reasons, contain details of the Regulator issuing the measure, and refer to the right of an effective remedy.⁸⁷¹

The HIPCAR Privacy Framework also notes the importance of independence where data controllers may be public or quasi-public sector organisations over which the executive can exercise administrative oversight. It enables the Data Commissioner to report to the Minister on the status of privacy protection by the private sector, and to the parliament on the status of privacy protection measures by the public sector.⁸⁷²

9.5.1 Penalties

All the Specified Frameworks other than the Commonwealth Bills allow Regulators to impose a variety of sanctions. Depending on the framework and the relevant facts, these range from administrative fines and sanctions to temporary and permanent bans regarding the processing of personal data.

The Commonwealth Bills are unique in this regard and allow the Privacy Commissioner to only submit recommendations to controllers. If the Privacy Commissioner finds non-compliance in the course of periodic investigations to check compliance, they must provide a report to the relevant controller with

866 Malavika Raghavan, Beni Chugh and Nishanth Kumar, 'Effective Enforcement of a Data Protection: A Model for Risk-Based Supervision Using Responsive Regulatory Tools', 18 (Dvara Research, 1 November 2019) <https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>.

867 'OECD best practices for regulatory policy' ch 2 (OECD iLibrary), p54 https://read.oecd-ilibrary.org/governance/the-governance-of-regulators/chapter-4-accountability-and-transparency_9789264209015-9-en#page1.

868 See the discussion on the requirement for agencies in the UK and US to publish Enforcement Manuals which are meant to provide information on the agencies' processes and enforcement powers in Trishee Goyal and Renuka Sane, 'Towards Better Enforcement by Regulatory Agencies' (2020) Data Governance Network Working Paper 14, 27 <https://datagovernance.org/report/towards-better-enforcement-by-regulatory-agencies>.

869 Trishee Goyal and Renuka Sane, 'Towards Better Enforcement by Regulatory Agencies' (2020) Data Governance Network Working Paper 14, 20 <https://datagovernance.org/report/towards-better-enforcement-by-regulatory-agencies>.

870 GDPR, art 58(4).

871 GDPR, recital 129. This would include a judicial review in the State that the supervisory authority that adopted the decision.

872 Explanatory Report to HIPCAR Model Legislative Text, para 71.

findings and recommendations. These documents may also be included in the annual reports that the Commissioner is required to submit to parliament. The complainant is entitled to seek judicial review if private organisations or state entities decide not to implement the recommendations of the Privacy Commissioner.⁸⁷³ However, the Commissioner's ability to enforce the regulatory framework is extremely limited if they are not given the power to impose penalties, beyond issuing recommendations and including findings in reports to the parliament.

9.5.2 Warnings, fines, and compensation

The sanctions that the other Specified Frameworks provide for are explored below.

Warnings and fines

The GDPR, Convention 108+ and the AU Convention specifically provide Regulators the power to impose sanctions and fines.⁸⁷⁴ Moreover, Convention 108+ specifies that authorities must, at a minimum, be provided with the power to issue decisions with respect to the regulatory framework's violations.⁸⁷⁵ This could involve imposing administrative sanctions, including fines. If a domestic legal system does not allow the supervisory authority to impose administrative sanctions, they could be applied in such a manner that the Regulator recommends the sanctions which are then imposed by courts.⁸⁷⁶ It should be noted that the sanctions imposed would have to be effective, proportionate, and dissuasive.

Compensation

The GDPR and Convention 108+ discuss compensation. The GDPR, however, is the only framework that specifically provides that pursuance of compensation is a right held by the data subject. It also specifies how the liability of various controllers and processors

would be determined and the circumstances under which they may be exempt from liability.⁸⁷⁷ Convention 108+ also specifies that compensation may be considered where applicable.⁸⁷⁸

The GDPR provides that data subjects have the right to mandate certain non-profit organisations to file complaints and receive compensation on their behalf. States may also provide by law that such organisations independently have the right to lodge complaints with the supervisory authority if it considers that data subjects' rights have been infringed.⁸⁷⁹ Overall, these measures can make it easier for data subjects to exercise their rights.

9.5.3 Directions

The GDPR, Convention 108+, HIPCAR Privacy Framework and the AU Convention provide Regulators with powers to direct a range of actions, such as rectification or erasure of relevant personal data, communicating these actions to the data subjects, and ordering temporary or permanent processing bans. These can prevent continuing violations of the frameworks and help protect data subjects' rights.

Directing compliance

The GDPR allows supervisory authorities to order controllers or processors to bring their processing operations into compliance with the regulatory framework and to comply with data subject requests to exercise their rights, as well as to communicate breaches of personal data to data subjects.⁸⁸⁰ The HIPCAR Privacy Framework provides for the use of enforcement notices as a tool for Data Commissioners to exercise their powers. When the Commissioner is of the opinion that a data controller has contravened or is contravening provisions of the framework, they may serve an enforcement notice requiring the controllers to take specified steps within specified timelines so that the violation is rectified.⁸⁸¹

873 Commonwealth Privacy Bill, Part IV, s 29 and 30; Commonwealth PPI Bill, s 36 and 37.

874 GDPR, arts 58(2)(a), 58(2)(b), and 58(2)(i); AU Convention, arts 12(2)(h), 12(3), and 12(4).

875 Convention 108+, art 15(2)(c), Explanatory Report to the Convention 108+, para 119, p 29.

876 Explanatory Report to the Convention 108+, para 119, p 29.

877 GDPR, art 82.

878 Explanatory Report to the Convention 108+, para 100, p 27.

879 GDPR, art 80. These organisations must be constituted in accordance with law, have statutory objectives that are in the public interest, and be active in the field of protection of data subjects' rights.

880 GDPR, arts 58(2)(c), 58(2)(d), and 58(2)(e).

881 HIPCAR Model Legislative Text, s 67; s 68 specifies the details that such notices must contain and the actions that it can require the controller to undertake.

Rectification, erasure and processing restrictions

Under the GDPR, supervisory authorities can order rectification, erasure, or the restriction of personal data processing. They may also notify the recipients of the personal data (such as third-party processors) of such actions.⁸⁸² They are also empowered to impose temporary or permanent limitations, including bans on processing, and may withdraw previously issued certifications to controllers and processors. In addition, they may order the suspension of data flows to recipients in third countries or international organisations.⁸⁸³

The AU Convention provides that in emergencies where the processing or use of personal data results in a contravention of fundamental rights and freedoms or where a controller fails to comply with official warning letter, the National Protection Authorities may undertake certain actions, such as ordering the temporary or permanent discontinuation of processing, or blocking certain types of data from being processed.⁸⁸⁴

In addition to other measures, the HIPCAR Privacy Framework allows for enforcement notices that can require the data controller to rectify or delete relevant data, or supplement the personal data with statements related to the issue for which the notice was issued, as approved by the Regulator.⁸⁸⁵ Separately, when the Commissioner requests information during an investigation, but cannot obtain enough information to assess whether processing is lawful, they may prohibit the controller from processing information in any way other than storage.⁸⁸⁶

9.5.4 Criminal sanctions

Criminal sanctions are specifically provided for in only a few frameworks. The AU Convention requires states to impose criminal penalties for a wide range of actions from breaches and attacks on computer systems to facilitating access to or producing prohibited content.⁸⁸⁷ It requires states to take the necessary regulatory and legislative measures to impose criminal penalties for offences delineated in the framework.⁸⁸⁸ Based on the nature of the offences, the HIPCAR Privacy Framework provides for fines, imprisonment or for both as punishment for violations of the framework.⁸⁸⁹ It is also the only instrument that prescribes similar penalties for data subjects who make requests to access or correct personal data under “false pretences”.⁸⁹⁰ The GDPR holds that states should be able to institute rules on criminal penalties for violations.⁸⁹¹

Convention 108+ does not contain many details and provides discretion to states, but notes that interventions depending on domestic law can take different forms, such as rectification or deletion of inaccurate data, issuing opinions as well as acting against non-compliant controllers. It also allows states to determine the nature of judicial and non-judicial sanctions, whether they are civil, administrative, or criminal actions. It requires the sanctions to be effective, proportionate, and dissuasive and also provides that financial compensation may also be considered where applicable.⁸⁹²

882 GDPR, art 58(2)(g).

883 GDPR, arts 58(2)(f), 58(2)(h), 58(2)(i) and 58(2)(j). They can also order the relevant certification body to withdraw certifications or not issue them if the requirements for certification are no longer met.

884 AU Convention, art 12(5).

885 HIPCAR Model Legislative Text, s 68(2).

886 HIPCAR Model Legislative Text, s 61.

887 AU Convention, arts 29-31.

888 AU Convention, arts 29(3)(2), 31(1).

889 See HIPCAR Model Legislative Text, Part VIII. This ranges from refusal to comply with the Commissioner’s requests for information or providing false or misleading information (s 60), breach of confidentiality obligations by the Commissioner or her staff or agents (s 56), controllers’ failure to comply with enforcement notices (s 69), performing any of the functions of a controller without being entered into the register maintained by the Commissioner (s 73); see also HIPCAR Model Legislative Text, Explanatory Notes, p 59, discussion on gradation based on the nature of offences.

890 HIPCAR Model Legislative Text, s 76.

891 GDPR, recital 149.

892 Explanatory Report to the Convention 108+, paras 100 and 121, pp 27 and 29.

Convention 108+, the GDPR, and the HIPCAR Privacy Framework also contain a more general provision allowing states to impose appropriate sanctions for contravention of the relevant framework.

9.5.5 Remedies

Data subjects can generally approach the Regulator and courts for remedy. Under each of the Specified Frameworks, data subjects can complain to the Regulator about data controllers' or processors' use of their personal data and other related actions.⁸⁹³ The GDPR provides data subjects the right to lodge a complaint with the supervisory authority and clarifies that it is without prejudice to other administrative and non-judicial remedies that are available to them.⁸⁹⁴

The GDPR also specifies that data subjects have the right to a judicial remedy if they consider that their rights under data protection legislation have been infringed upon by processors or controllers, or if the relevant supervisory authority does not handle a complaint or fails to inform them about the status of a complaint within three months after filing.⁸⁹⁵ Convention 108+ also notes the importance of data subjects to seek judicial remedy, regardless of whether the supervisory authority intervenes on their behalf in court to enforce their rights.⁸⁹⁶

More generally, Convention 108+ highlights the importance of specifying data subjects' rights, the obligations of controllers and corresponding sanctions and remedies in guaranteeing effective data protection. It specifies that it is left to each state to determine the nature of remedies but requires non-judicial remedies to be made available to data subjects. It also notes that financial compensation to affected data subjects for material as well as non-material damages could be considered.⁸⁹⁷

9.5.6 Appeals

Other than under the Commonwealth Bills, data subjects can appeal Regulators' decisions, usually before the courts under the Specified Frameworks.⁸⁹⁸ When receiving a complaint, the HIPCAR Privacy Framework also allows the Data Commissioner to authorise a mediator to investigate the appeal and try to arrive at a settlement.⁸⁹⁹

893 GDPR, arts 77,78,79 HIPCAR Model Legislative Text, p 62; AU Convention, art 12(2)(e); Commonwealth Privacy Bill, Part IV, s 23; Commonwealth PPI Bill, s 29.

894 GDPR, art 77(1).

895 GDPR, arts 78 and 79.

896 Explanatory Report to the Convention 108+, para 133, p 30.

897 Explanatory Report to the Convention 108+, paras 99 and 100, pp 26-27.

898 AU Convention, art 12(6); Convention 108+, art 15(9), and Explanatory Report to the Convention 108+, para 124, p 29; GDPR, art 78; HIPCAR Model Legislative, ss 47 and 81.

899 HIPCAR Model Legislative Text, s 42.

Key considerations

- ◇ The Identified Regional Frameworks provide varying levels of detail about the regulatory structure applicable to data protection. Nevertheless, the general approach is to establish a supervisory authority that is responsible for enforcing the data protection legislation and related functions. The functions and powers of Regulators range from the monitoring and enforcement of the data protection framework, authorising data processing, and providing information to handling complaints relating to data protection and conducting investigations.
- ◇ Regardless of the specific structure, it is essential for Regulators to be designed to be autonomous, and have the resources to function effectively so that they can operate independently and transparently. The composition of regulators, access to funding and resources, and the appointment, dismissal, qualifications/ disqualifications and tenure of its members, are some factors that impact the independence of regulators.
- ◇ Furthermore, regulators should be accountable to multiple stakeholders, and should be able to effectively coordinate with public authorities, regulators and private organisations, as well as with other supervisory authorities. They should also be empowered to impose penalties and hold both state and private actors accountable for noncompliance with data protection laws.

