PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

The Keys to Data Protection

August 2018

Contents

Introduction

The right to privacy is a fundamental right enshrined in many constitutions around the world, as well as in international human rights law. The right to privacy is multi-faceted, but a fundamental aspect of it, increasingly relevant to people's lives, is the protection of individuals' data.

As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring implementation of the International Covenant on Political and Civil Rights (ICCPR), recognised the need for data protection laws to safeguard the fundamental right to privacy recognised by Article 17 of the ICCPR.

Protecting privacy in the digital age is essential to effective and good democratic governance. However, despite increasing recognition and awareness of data protection and the right to privacy across the world, there is still a lack of legal and institutional frameworks, processes, and infrastructure to support the protection of data and privacy rights. At the same time, the increasing volume and use of personal data, together with the emergence of technologies enabling new ways of processing and using it, mean that regulating an effective data protection framework is more important than ever.

Protecting privacy is essential, and the majority of States have adopted some forms of protection; however, frameworks are often inadequate, and have not kept up with modern uses of data and challenges they pose. Data protection laws need to be updated to face emerging challenges.

For the last three decades, Privacy International has been promoting and advocating for the right to privacy and, through the Privacy International Network, we have been calling for the adoption and enforcement of the strongest data protection safeguards across the world.

Over the years, some of these issues have expanded and some entirely new ones have emerged: the dominant narratives we are challenging have evolved and new actors, both allies and adversaries, have entered our scope of intervention.

Data-Intensive Systems

Governments across the world are radically changing policies and infrastructure, in the hope of enabling economic opportunity and attracting international investment, ensuring the security of their societies, and strengthening institutions.

Governments are continuously developing new policies that demand more data from individuals: a vast change in the relationship between the individual and the State through the accumulation of data. It is not just about government, industry plays an essential role too: they promote the ideas, support the sales of such systems, and

provide the tools and services. They may also control the data. This all results in what we call *data-intensive systems*. These are systems which process data about people, which generate additional data about people, and which rely on data to make decisions about people.

With data-intensive systems, too-often governments and industry see new opportunities: for surveillance, income generation, and control. There are few safeguards in place. The drive for these changes is strongest in emerging economies where legal and technical safeguards are weakest and there is little to no transparency of decision-making processes, and limited rule of law, and the responsibilities of the private sector are blurred. What we are seeing is that innovations in policy and technology are largely left unregulated and unchecked. This will have significant ramifications for privacy, and will transform the exercise of power, creating new possibilities for oppression, strengthening existing inequality, discrimination, and exclusion, and potentially leading to new forms.

There are also systemic structural challenges. There is often little or no public consultation, transparency of resource-allocation, and oversight or audits of how these systems are functioning. Additionally, governments are increasingly relying on industry to deploy systems and run software; equally, industry are becoming dependent on governments sanctioning access to data. In this way, the separation between government and industry will blur, and this will fuse their respective duties and obligations.

To find out more about our work on data-intensive system visit the PI website.

Data Exploitation

Increasingly, everything we do generates data, whether we are in possession of a device or not. Our devices, networks, and even homes generate vast amounts of data. Our transport systems, cars, payment systems, and cities also generate data through us and about us. With all this data, we may be able to make the world a fairer, better, cleaner, more sustainable, and safe place. The opposite may also be true.

Our devices and infrastructure are being designed for data exploitation. Increasingly, it is beyond the ability of individuals themselves to control the ways in which data about their lives is shared and processed.

As a result, industry and government are amassing our data with impunity. They aspire to a data-driven world which frees them to grab our data, to look for patterns and similarities, to generate intelligence, and to make decisions about us and the shape of our futures.

We are not ready for the future which is already being built. Our laws are not yet able to address these risks. Our technologies are insecure and leak data. In turn, we ourselves are not secure.

To find out more about our work on data exploitation visit the Privacy International website.

Why We Wrote This Guide

Through our global work including with the Privacy International Network, Privacy International has observed the discrepancies and shortcomings of data protection across the globe:

- Some countries around the world still don't have comprehensive data protection law, but around 40 have initiated a legislative process, and have a bill in the process of being drafted;
- Those with data protection laws often lack effective implementation and enforcement or have not updated their legislation to address current uses (and abuses) of personal data; and
- Comprehensive data protection laws provide the main legal framework, including the principles, rights, and sanctions regimes to protect personal data. Other sectoral legislation may also be needed (e.g. in the field of telecommunications) to complement the general data protection framework.

Given the diversity of the legal landscape, our interventions require us to be engaged in both the drafting of new laws as well the reform of existing ones, as well as being vigilant as to the implementation and enforcement of such frameworks.

In addition, Privacy International has noted that there is a systemic problem: limited or absent civil society engagement, as well as among other non-state stakeholders, in these policy processes. This is often not out of a lack of interest of civil society organisations (CSOs), but is the result of structural and institutional challenges, such as the lack of expertise on these issues within CSOs or, importantly, the lack of opportunity to engage - policy development often happens in the shadows, behind closed doors.

National CSOs across the world must be part of policy development and consultation in relation to data protection, in order to articulate the protection and safeguards needed, and ensure that process is inclusive, open, and transparent. Repeatedly, our experience has shown that the more CSOs (from across disciplines) are involved in these policy processes, the better-informed actors of change are, and the greater policy discourse there is: ultimately the aspiration is laws and policies uphold, respect and promote fundamental rights.

This guide was developed to support these efforts and strengthen the global campaign for effective data protection.

About this Guide

This guide was developed from Privacy International's experience, expertise on international principles and standards applicable to the protection of privacy and personal data, and leadership and research on modern technologies and data processing.

The guide is intended to help with the analysis of a data protection law, be it:

- a white paper (to inform the development of a law);
- a bill (a draft proposed law);
- an existing law; or
- a proposal for amending existing data protection regimes.

The guide is structured to provide a coherent and efficient analytical process by addressing in turn the various provisions which are commonly presented in a data protection law.

This guide does not provide an exhaustive list of all the ideal provisions of a data protection law, but instead focuses on areas which, in our experience, have required further engagement and guidance to ensure that the law upholds a country's national and international human rights obligations to protect the right to privacy and other fundamental rights, as well as complying with international and regional data protection standards and principles.

Each section provides some background information about what the regulatory objective is, the different elements it should contain, and (where relevant) some guidance and language to support the crafting of both general and specific comments.

The guide references examples from around the world. There is a strong focus on examples from the European Union data protection framework, as one of the most recent and comprehensive frameworks, as well as regional and international guidelines and treaties. This guide is for CSOs around the world, and can be adapted to suit different national frameworks and local contexts.

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 1:

Data Protection, Explained

Data Protection, Explained

What is Data Protection?

Data protection is commonly defined as the law designed to protect your personal data. In modern societies, in order to empower us to control our data and to protect us from abuses, it is essential that data protection laws restrain and shape the activities of companies and governments. These institutions have shown repeatedly that unless rules restricting their actions are in place, they will endeavour to collect it all, mine it all, keep it all, share it with others, while telling us nothing at all.[1]

Why is Data Protection Needed?

Every time you use a service, buy a product online, register for email, go to your doctor, pay your taxes, or enter into any contract or service request, you have to hand over some of your personal data. Even without your knowledge, data and information about you is being generated and captured by companies and agencies that you are likely to have never knowingly interacted with. The only way citizens and consumers can have confidence in both government and business is through strong data protection practices, with effective legislation to help minimise state and corporate surveillance and data exploitation.

Since the 1960s and the expansion of information technology capabilities, business and government have been storing this personal data in databases. Databases can be searched, edited, cross-referenced, and their data shared with other organisations across the world.

Once the collection and processing of data became widespread, people started asking questions about was happening to their data once they provided it. Who had the right to access the data? Was it kept accurately? Was it being collected and disseminated without their knowledge? Could it be used to discriminate or violate other fundamental rights?

From all these questions, and amid growing public concern, data protection principles were devised through numerous national and international consultations. The German region of Hesse passed the first law in 1970, while the US Fair Credit Reporting Act 1970 also contained elements of data protection.[2] The US-led development of a 'code of fair information practices' in the early 1970s continues to shape data protection law today. At around the same time, the UK established a committee to review threats by private companies, which came to similar conclusions.

National laws emerged soon afterwards, beginning with Sweden, Germany, and France. As of January 2018, over 100 countries had adopted data protection laws, with pending bills or initiatives to enact a law in a further 40.[3]

Over time, regional legal frameworks were also adopted. In 1980, the Organisation for Economic Cooperation and Development (OECD) developed its guidelines, which included 'privacy principles'; shortly afterwards, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data entered into force - this was modernised in 2018.[4]

The sheer volume of data generated and the rapid development of technology, including sophisticated profiling and tracking, and artificial intelligence, means that some existing data protection laws are out of date and unfit to deal with processing as it currently functions. Frameworks fail to reflect the new potential for data processing which emerged with advancement of technologies which were deployed and embedded within governance systems and business models.

It has been reported that 90% of data in the world today was created in the last two years, and every two days we create as much data as we did from the start of time until 2013[5]. When many data protection frameworks were drafted the world was a very different place. For example, many laws were adopted before Google, Facebook or smartphones were even created, let alone widely used.

A data protection framework may have its limitations (which we are trying to identify and address by exploring what other regulations are needed to provide the necessary safeguards) but it does provide an important and fundamental starting point to ensure that strong regulatory and legal safeguards are implemented to protect personal data.

A strong data protection framework can empower individuals, restrain harmful data practices, and limit data exploitation. It essential to provide the much-needed governance frameworks nationally and globally to ensure individuals have strong rights over their data, stringent obligations are imposed on on those processing personal data (in both the public and private sectors), and strong enforcement powers can be used against those who breach these obligations and protections.

Data Protection: Essential for Exercise of Right to Privacy

Privacy is an internationally recognised human right. Article 12 of the Universal Declaration of Human Rights (UDHR) proclaims that

> **[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence .... Everyone has the right to the protection of the law against such interference or attacks.** [6]

The UDHR has formed the basis for the major international human rights treaties, which similarly enshrine the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR) in Article 17.

As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring implementation of the ICCPR, recognised the need for data protection laws to safeguard the fundamental right to privacy recognised by Article 17 of the ICCPR:

> **The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. ... [E]very individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files ... have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination** [7]

In 2011, the then-UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report similarly noting that "the protection of personal data represents a special form of respect for the right to privacy."[8] The report further noted that:

> **[t]he necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over information of their users.** [9]

And in 2013, he also noted that the right to privacy includes:

> **the ability of individuals to determine who holds information about them and how [...] that information [is] used.**[10]

In December 2016, the UN General Assembly passed a resolution (by consensus) on the Right to Privacy in the Digital Age, GA Res. 71/199, which reaffirmed previous General Assembly resolutions on the subject, emphasising that:

> **States must respect international human rights obligations regarding the right to privacy [...] when they require disclosure of personal data from third parties, including private companies.**[11]

Privacy and data protection are intrinsically linked. Individuals, as citizens, customers, and consumers, need to have the means and tools to exercise their right to privacy and protect themselves and their data from abuse. It is also important that the obligations of those processing data are clear, so that they take measures to protect personal data, mitigate interference with the right to privacy, and are held to account when they fail to comply with obligations. This is particularly the case when it comes to our personal data. Personal data, as described below in detail, is data (information processed by automated means or kept in a structured filing system) which relates to an individual. Data protection is about safeguarding our fundamental right to privacy by regulating the processing of personal data: providing the individual with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

Data Protection: A Right?

The protection of personal data has long been recognised as a fundamental aspect of the right to privacy. In recent years it has been recognised as a standalone right. For example, data protection has been included as a standalone right under the Charter of Fundamental Rights of the European Union (2012/C 326/02) under Article 8 (in addition to Article 7 of the Charter which upholds the right to privacy). Article 8 reads:

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

In many countries around the world, there is a Constitutional right of habeas data, which is designed to protect the data of an individual by granting them the right to access the information held about them, and providing for the individual concerned to submit a complaint to the Constitutional Court.

Article 5, 1988 Brazilian Constitution:
Habeas Data shall be granted: a) to ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative.

Article 15, Constitution of Colombia, as amended in 1995:
All individuals have the right to personal and family privacy and to their good reputation, and the State has to respect them and to make others respect them. Similarly, individuals have the right to know, update, and rectify information collected about them in data banks and in the records of public and private entities.

Freedom and the other guarantees approved in the Constitution will be respected in the collection, processing, and circulation of data.

Correspondence and other forms of private communication may not be violated. They may only be intercepted or recorded on the basis of a court order in cases and following the formalities established by law.

For tax or legal purposes and for cases of inspection, the oversight and intervention of the State may demand making available accounting records and other private documents within the limits provided by law.

How Does Data Protection Work?

There are no universally-recognised data protection standards, but regional and international bodies have created internationally-agreed-upon codes, practices, decisions, recommendations, and policy instruments.

The most significant instruments are:

- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 as amended in 2018
- The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) as amended in 2013
- The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

Other regional frameworks also exist including the APEC Privacy Framework - Asia-Pacific Economic Cooperation.[12]

Where a comprehensive data protection law exists, organisations (public or private) that collect and use your personal data, have the obligation to handle this data according to the data protection law.

Data protection should ensure the following:

- There should be limits on the collection of personal data, and it should be obtained by lawful and fair means, as well as being done in a transparent manner
- The purposes for which the data and information is to be used should be specified (at the latest) at the time of collection, and should only be used for those agreed purposes. Personal data can only be disclosed, used, or retained for the original purposes (i.e. the purpose at the time of collection), except with the consent of the individual or under law: accordingly, it must be deleted when no longer necessary for that purpose
- Personal data, as generated and processed, should be adequate, relevant, and limited to necessity of the purposes for which it is to be used
- The data should be accurate and complete, and measures should be taken to ensure it is up to date
- Reasonable security safeguards should be used to protect personal data from loss, unauthorised access, destruction, use, modification, or disclosure
- There should be no secret processors of data, sources, or processing. Individuals must be made aware of the collection and processing of their data, as well as the purpose of its use, who is controlling it, and who is processing it
- Individuals have a range of rights which enables them to control their personal data and any processing
- Those that use personal data must be accountable for and demonstrate compliance with the above principles, and facilitate and fulfil the exercise of these rights, abiding by applicable laws that enshrine those principles

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, as amended by 2018

Article 5 (4):
Personal data undergoing processing shall be:
a. processed fairly and in a transparent manner
b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further

processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes
c. adequate, relevant and not excessive in relation to the purposes for which they are processed
d. accurate and, where necessary, kept up to date
e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed

General Directive Personal Data, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Principles presented in Article 5:
1. Lawfulness, fairness and Transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Accountability should be at the core of any law regulating of the processing of personal data and the protection of the rights of individuals, and data protection rules thus need to be enforced by a regulator or authority. The strength of powers invested in these authorities varies from country to country, as does their independence from government. Some jurisdictions have established more than one regulatory body for oversight regulation and enforcement, with powers depending on if the data is being processed by public or private entities, e.g. Colombia. These powers, for example, can include the ability to conduct investigations, act on complaints, and impose fines when an organisation has broken the law.

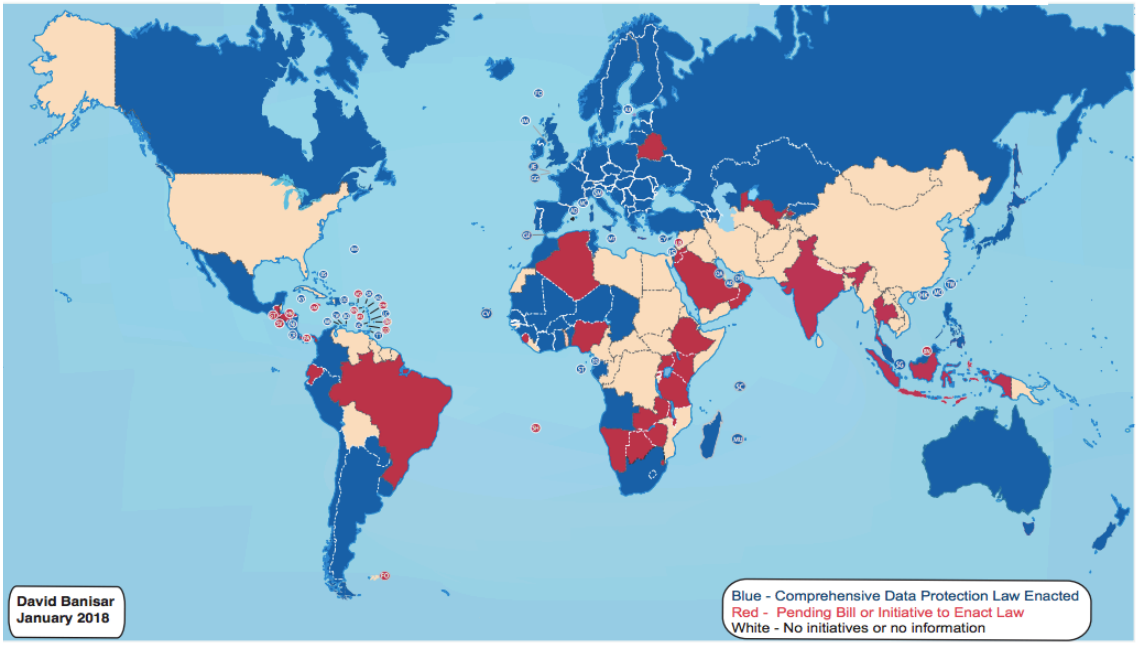
Redress for breaches of data protection law should also be available through the courts, both through individual actions and collective redress (brought by NGOs and consumer groups).

In summary, data protection works through key principles which give individuals rights over their data: those that process data have obligations in relation to the data, and enforcement and redress must be available when these principles, rights and obligations are not adhered to.

Data Protection in Practice Today

As of January 2018, over 100 countries around the world have enacted comprehensive data protection legislation, and around 40 countries are in the process of enacting such laws. Other countries may have privacy laws applying to certain areas, for example for children or financial records, but do not have a comprehensive law on data protection.

National Comprehensive Data Protection/Privacy Laws and Bills 2018



Source: Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (January 25, 2018). Available at SSRN:https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

In countries where there is no comprehensive data protection framework, data protection is regulated through sectorial laws where it is regulated at all. For instance, though an early leader in the field of data protection, the US Privacy Act 1974 applies only to the Federal Government, and subsequent laws apply to specific sectors or groups of individuals (e.g. the Children's Online Privacy Protection Act (COPPA)), but there is no comprehensive data protection law to date. This sectorial approach is still in place in many countries, including India.

A significant development in data protection law occurred with the adoption of the EU General Data Protection Regulation (GDPR), which will take effect on 25 May 2018. The GDPR is comprehensive, covering almost all personal data processing. It is also significant, as its implementation will affect not only data controllers based within the EU, but also those that offer goods or services to, or monitor the behaviour of, individuals based in the EU.

In May 2018, there was a further development with the amendment of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108). Since its adoption in 1981, over 40 European countries and nine non-Members of Council of Europe have used the Convention as a foundation of their own data protection frameworks. The modernised text of the Convention reaffirms existing principles, and adopts new provisions to strengthen obligations, accountability, and enforcement mechanisms. [13]

For more information on data protection laws, broken down by country, see Privacy International's comprehensive reports. [14]

Data Protection: A Piece of the Puzzle

In protecting the right to privacy of individuals as well as their data, data protection is only a piece of the puzzle.

A general data protection framework does not preclude the adoption or application of sectoral laws regulating particular sectors. Any data protection law should make it clear that its scope is to protect the fundamental rights of individuals, such as the right to privacy and personal data protection, and therefore any laws (current or future) which contradict such protection, e.g. by limiting those fundamental rights, should be considered null and void.

There is a need to ensure that necessary legislation be adopted to regulate government and private sector policies and practices which interfere with the right to privacy and entail the processing of personal data. These could include laws regulating, but are not limited to:

- Communications surveillance
- Information and technology
- Law enforcement
- Trade
- Education
- E-governance
- Health care services
- Financial and banking institutions
- Consumer protection
- Cyber-security
- Product liability

These should ensure the protection of the individual and their data as well as respect their right to privacy.

A Step-by-Step Guide to Data Protection

While data protection laws vary from country to country, there are some commonalities and minimum requirements, underpinned by data protection principles and standards.

Laws tend to have some general provisions providing for:

- The scope of the law
- Definitions
- Data protection principles
- The obligation of controllers and processors
- The rights of data subjects
- Oversight and enforcement

The different chapters of the guide outline and explain these general provisions in more detail, presenting the key components of data protection through a variety of national and global examples.

References

1 See full text: https://www.privacyinternational.org/explainer/41/101-data-protection

2 Robert Gellman, 'Fair Information Practices: A Basic History', April 2017, available [PDF] at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

3 David Banisar, 'National Comprehensive Data Protection/Privacy Laws and Bills 2018', available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 (last revised 25 Jan 2018)

4 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 128th Session of the Committee of Ministers, 18 May 2018, CM(2018)2-final. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

5 Thomas A Singlehurst et al, 'ePrivacy and Data Protection', CitiGroup, March 2017, p4. Available (PDF) at https://www.citibank.com/commercialbank/insights/assets/docs/ePrivacyandData.pdf

6 GA Res. 217 (III) A, UDHR, art. 12 (Dec. 10, 1948)

7 UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, para 10.

8 UN Doc. A/HRC/17/27, para 58 (May 16, 2011).

9 Id. para 56

10 UN Doc. A/HRC/23/40, ¶ 22 (Apr. 17, 2013).

11 GA Res. 71/199, at 3; accord Human Rights Council Res. 34/7.

12 APEC Privacy Framework, December 2005, available at https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

13 Council of Europe, 'Modernisation of Convention 108', Council of Europe Portal, available at https://www.coe.int/en/web/data-protection/convention108/modernised

14 Privacy International, 'State of Privacy', available at https://www.privacyinternational.org/reports/state-of-privacy

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 2:

General Provisions, Definitions and Scope

General Provisions, Definitions and Scope

General Provisions

Object and purpose of the law

This section should provide a legitimate aim or purpose of the law. It is good practice that this section of the law would make direct reference to fundamental rights and international human rights obligations, and the State's responsibilities under national and international law, and explicitly confirm that this law would comply with these in its scope and application.

The following should be included:

1. Reference to the right to privacy and/or protection of personal data, as upheld by the Constitution, if applicable.
2. Reference to international and human rights obligations as upheld by regional and international treaties to which the country is a signatory, as applicable:
    - The International Covenant on Civil and Political Rights (ICCPR) 1966
    - The American Convention on Human Rights
    - The American Declaration of the Rights and Duties of Man
    - The Arab Charter on Human Rights
    - The ASEAN Human Rights Declaration
    - The European Convention on Human Rights
    - The EU Charter on Fundamental Rights and Freedoms
    - The African Charter on Human and People's Rights
    - The African Charter on the Rights and Welfare of the Child
    - Other, as applicable.
3. Reference to regional and international instruments on data protection which may be legally binding or not:
    - the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
    - the Council of Europe Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, as amended in May 2018
    - the EU General Data Protection Regulation and the EU law enforcement directive
    - the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004

- the Economic Community of West African States has a Supplementary Act on data protection from 2010;
- the African Union Convention on Cyber Security and Personal Data
- Other, as applicable.

The inclusion of these references is necessary for legal purposes, associating the protection of a personal data with a right which, if interfered with or violated, can result in harming those affected. This approach also serves as a means of humanising data protection law: when drafting laws and policies, it is often forgotten that those affected by the law are not just 'subjects of the law' or 'data subjects' but individuals. In terms of the discourse, a human or civil rights approach is essential and beneficial to ensure a constructive framing of these policy processes.

Object of Convention 108 modernised to protect individuals

A shift in thinking around the role and purpose of data protection is illustrated by the May 2018 amendment to the Convention 108 which reframed to focus on the protection of the individual, their data, and their fundamental rights:

> **"The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and particular the right to privacy."**

Definitions

The most fundamental and recurrent terms in the law must be clearly defined at the outset.

Our experience has been that there are particular terms and definitions which must be provided for in legislation, but which are often missing or are incorrectly or poorly defined, including in relation to what and who the law applies to. The definitions below seek to address common shortcomings.

Personal data

With recent evolution of data processing mechanisms as a result in advancement of technology, as well as increased intelligence and information which can be gathered from raw data, it is essential that a clear and comprehensive definition of 'personal data' is provided for in the law, as it is on the basis of that definition that the law will be applied. The terminology can vary and in some countries, such as the U.S.A, personal data is referred to as 'personally identifiable information.'

In general, it is common for the definition of personal data to be relatively broad, however, occasionally the definition is limited in scope, and it fails to consider e.g. further processing, or data that can indirectly identify a person.

An example definition from the EU GDPR is:

> **"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (GDPR)"**

<u>The Evolution of What Constitutes Personal Data</u>

There is a need for an evolved and expansive definition 'personal data' – it must include any data which can be used to identify an individual, directly or indirectly. The types of identifiers will develop with technology, for example, it is now widely recognised that an IP address is personal data.

In October 2016, the European Court of Justice (ECJ) judged that the term 'personal data', "must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."

Furthermore, there are methods of data processing (such as profiling, tracking, and monitoring) which do not require a specific name/address or other direct identifier in order to identify individuals, and affect how they are treated. Indirect identification is a key element to be included in the definition of personal data.

In the era of data linkability, and de-anonymisation of data sets, and with the development of artificial intelligence, there are also concerns that other forms of data can become personal data, as they can lead to an individual being uniquely identified and identifiable. The signature of movements and device identifiers, including behaviour using the device, can be linkable between non-sensitive and sensitive transactions. Any definition in legislation should take into account that personal data can be revealed from other data, it can be derived, inferred and predicted.

Examples of personal data

- a name and surname
- a home address
- an email address such as name.surname@company.com
- an identification card number
- location data (for example the location data function on a mobile phone)*
- an Internet Protocol (IP) address
- a cookie ID*
- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Source: European Commission, What is personal data? Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Sensitive personal data

It is common for certain categories of personal data to be distinguished on the grounds that they are 'sensitive', or a special category, which, when processed, requires additional levels of protection. This category of data attracts higher safeguards, including limitations on the permitted grounds for processing it.

Most laws do not provide a definition, but instead give a list of data which constitutes sensitive personal data, or a list of special categories of personal data. However, in some jurisdictions, such as in Colombia, provisions on sensitive personal data refer to data which may impact the privacy of the individual, or date whose undue use may result in discrimination.[1]

In general, categories of data identified as sensitive can be related to the types of discrimination addressed in human rights instruments and constitutional protections enshrine the right to non-discrimination.[2]

There is no exhaustive list of what constitutes sensitive personal data. However, data pertaining to the following information has become widely regarded as constituting sensitive personal data:

(a) the racial or ethnic origin of the individual
(b) political opinions
(c) religious or philosophical beliefs or other beliefs of a similar nature
(d) membership of a trade union
(e) physical or mental health
(f) sexual orientation
(g) the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
(h) biometric data [3]
(i) genetic data.[4]

Consideration should be given to other categories which might be included, for example, financial data, social security numbers, and data relating to children. Some countries have also discussed the possibility of adding other categories of data requiring additional protection because of its 'sensitivity' within their own national context. For example, in India, treating 'caste information' as sensitive personal data was.[5] Seeing governments consider local context and realities is an important step in ensuring that relevant safeguards are provided for in legislation.

It is also important that the higher protections extend to data which reveals sensitive personal data, through profiling and the use of proxy information (for example, using someone's purchase history to infer a health condition), it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data.

Processing

Some definitions of processing will fall short of providing for the breadth and scope of 'processing' and are limited to collection.

The definition of 'processing' should be broad and inclusive, rather than exhaustive. This would encourage countries to think innovatively and progressively in response to technological advancements in data analysis methods.

Processing should cover the entire 'lifecycle' of data - from its creation to its deletion - as well as the use of data to reveal other data.

> **"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[6]**

With this in mind, Privacy International proposes the idea of specifically integrating the generation of data within the definition of processing. It is an activity which has so far not been explicitly addressed within data protection law, and it must be regulated and overseen, and for which individuals must be awarded protection.

This suggestion is based on Privacy International's analysis that the problems with what we have called 'data exploitation' often begin with excessive generation, since generation is the precondition for further processing. This excessive generation of data by the systems and services we use, together with root causes such as lack of awareness, transparency and accountability lead to the core problem of power imbalances in a data driven world. This addition to the definition of 'processing' would complement the 'use limitation principle' and concept of 'data minimisation'.

Data controllers and data processors

Accountability and enforcement are key to the success of the protection of personal data. The law should clearly identify the parties responsible for complying with the law, as well as their obligations and duties.

Over time, there has been an evolution in the terminology used to refer to those responsible and accountable for the processing of personal data. While terminology varies across different data protection frameworks, there are two entities which have control over personal data and/or process personal data, known as data controllers and processors respectively.

Data controllers are a natural or legal person, public or private, that, by itself or in association with others, decides the purposes and means of the processing of personal data i.e. the 'why' and 'how'.

Data processors are a natural or legal person, public or private, that by itself or in association with others, performs the processing of personal data on behalf of the data controller i.e. often limited to technical solutions, the 'methods and means' of processing.

Profiling

This is a relatively new term but it is essential that 'profiling' be given explicit recognition within data protection law, given the use of data to derive, infer, and predict other information about individuals, and the challenges resulting from data mining and machine learning, among other innovative data techniques.

The following definition of profiling is included in both the Philippine's Data Privacy Act 2012 (section 1.(p)) and the GDPR (Article 4(4):

> **"Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."**[7]

Scope and Application of the Law

Material scope

What should the regulation apply to?

The law should apply to the automated data and automated data processing and structured formats of storing manual data. This means that a data protection law should cover any processing of data on a computer, on a phone, on an Internet of Things (IoT) device, and also via paper records.

The suggested scope of application, as seen in Article 2(1) of the GDPR, is:

> **“any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.”**

A filing system is defined further in Article 4(6):

Public and private institutions: two entities, two regulations

Some countries have chosen to have two (or more) separate pieces of legislation applying at the national level to government and private companies. This is the case of Canada and Mexico, for example. In the European Union, there is a separate piece of legislation for authorities processing personal data for law enforcement purposes.

Privacy International recommends that a comprehensive data protection law applies to public and private bodies. In no circumstances should public or private bodies be completely exempted from data protection principles, respecting the rights of individuals, or independent monitoring and enforcement.

Who should the regulation apply to?

It is essential that this section of any law provides clarity as to whom the law applies. Data protection legislation should apply to both public and private institutions. It is unacceptable practice that public institutions (including law enforcement and intelligence agencies) be completely exempt from having obligations to protect the personal data of data subjects, or for exemptions to be excessively wide or vague.

Along with limiting scope of the law to 'natural persons', it is widely accepted that processing for domestic or household purposes is exempt from application. Some jurisdictions include further criteria for this exemption. In an online world, where the lines between professional and personal are increasingly blurred, consideration should be given to how this exemption is defined and explained to data subjects.

Examining Exemptions

It is very common for governments to introduce exemptions from obligations and individual rights. The most recurring reasons are:

- **national security**
- **defence**
- **public security**
- **the prevention, investigation, detection or prosecution of criminal offences**
- **public interests**
- **immigration**
- **economic or financial interests, including budgetary and taxation matters**
- **public health and security**
- **the protection of judicial independence and proceedings**
- **monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime prevention**
- **the protection of the individual, or the rights and freedoms of others**
- **the enforcement of civil law matters.**

Blanket exemptions are never justifiable. In the limited cases where an exemption is justifiable, it should only apply in limited circumstance. It is essential to ensure that any exemptions are:

1. **clearly defined and prescribed by law**
2. **respect individual's fundamental rights and freedoms,**
3. **are necessary and proportionate measure in a democratic society, and**
4. **are only applicable, where failure to do so prejudice the legitimate aim pursued.**

The OECD has emphasised that any exceptions to the protections included within a data protection law in the name of national sovereignty, national security and public order (ordre public), should be:

a) as few as possible,
b) made known to the public.

The law should specifically provide for the development and inclusion of standards

applicable to the protection of personal data which is collected and processed for the purposes of public safety, defence, state security and investigation or prevention of criminal offences.

These provisions should, at a minimum, identify the public bodies mandated to collect and process personal data, fully respect and protect the right to privacy, and comply with the principles of legality, necessity and proportionality identified by international human rights experts, all under the supervision of an external body

Exceptions

A common exception to the scope of a data protection law is the processing of personal data by security and intelligence agencies. It is thus essential to ensure that:

1. Any processing of personal data, including at rest (i.e. government managed databases), by security agencies, intelligence agencies and law enforcement is subject to data protection legislation.
2. The legislation is comprehensive and provides the highest standards of protection. Any exceptions should be limited, clearly outlined, precise and unambiguous, made public, and narrowly interpreted according to principles of necessity and proportionality. This approach to exceptions would ensure that the protections provided for in a data protection law are not rendered redundant in relation to the functions of security and intelligence agencies.

Failure to properly define and limit these exceptions will undermine public trust in data protection.

Human right mechanisms and CSOs express concern about intelligence-sharing

Non-transparent, unfettered and unaccountable intelligence-sharing threatens the foundations of the human rights legal framework and the rule of law. The regime of transfer of personal data outside the national territory by intelligence services must be provided for, and (at least) brought into line with the regime of international transfers of personal data contained elsewhere in the law.

The European Court of Human Rights has expressed concerns regarding intelligence-sharing and the need for greater regulation and oversight:

> **The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance ... is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.**

In reviewing the UK's implementation of the International Covenant on Civil and Political Rights, the UN Human Rights Committee has specifically noted the need to adhere to Article 17, "including the principles of legality, proportionality and necessity," as well as the need to put in "effective and independent oversight mechanisms over intelligence-sharing of personal data."

In the UK, the Data Protection Act 2018 fails to regulate cross-border sharing of personal data by intelligence services. The relevant section gives almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection.

Privacy International, along with other human rights organisations, has called for greater accountability, transparency, and oversight of intelligence sharing agreements. Any exception for intelligence services should be narrowly construed within the law, as well as necessary and proportionate to a legitimate aim; these agreements should be subject to data protection legislation.

Territorial scope of application

Modern data protection law needs to take into consideration that data, including personal data, travels across borders. This raises significant and complex jurisdictional issues, including possible clashes of applicable national laws. Privacy International believes that data protection law should put individuals at its centre: this means ensuring that the personal data of the individual is protected, irrespective of whether their data is processed within or outside the territory where they are based.

This protection can be achieved in a variety of ways, including by providing that the law:[8]

- Applies to controllers and processors established in the country, even if the processing takes place outside the jurisdiction of the country
- Applies to the processing of personal data by controllers and processors established outside the jurisdiction of the country where the individual is based
- Regulates the conditions for transferring of personal data outside the territory of the country.

Territorial scope and application of a data protection law can be unclear and has often been interpreted very narrowly, construed to apply only where the data processing was taking place, i.e. interpreted to apply only to entities based in a particular jurisdiction, which could be used by companies to avoid offering protections to users.[9] However, given globalised infrastructure, it is no longer appropriate to think of data protection being confined by the boundaries of national territory: data protection frameworks have started to push interpretation towards extra-territorial application, so that individuals are not deprived of protections they are entitled to because of where the controller or processor is based.

For example, included within the scope of the GDPR under Article 3 are controllers/processors offering goods or services to individuals in the EU, or monitoring the behaviour of individuals in the EU (including online tracking).

Legislators have an obligation to protect the rights of those in their jurisdiction, including the right to privacy and data protection. Therefore, in order that individuals are not deprived of the protections they are entitled to, data protection frameworks should be clear as to how the law applies and protects individuals in each of these scenarios:

- The data controller/data processor is established in the relevant jurisdiction, even if processing takes place elsewhere
- The controller or processor is not established within that jurisdiction, but is processing personal data of an individual in that jurisdiction
- The data is transferred to a third party outside that jurisdiction.

References

1 Article 5 of the Law 1581 of 2012 of Colombia

2 One example is the article 2, paragraph 2 of the International Covenant on Economic, Social and Cultural Rights, as interpreted in the General Comment No. 20: Non-dicrimination in economic, social and cultural rights. Available at: http://www.refworld.org/docid/4a60961f2.html

3 biometric data' is personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, , Article (4) (14) of the EU GDPR.

4 'genetic data' is personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, Article (4) (13) of the EU GDPR.

5 White Paper of the Committee of Experts on a Data Protection Framework for India, Section 4.3, available (PDF) at: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf, pp. 43

6 This is the definition provided for within GDPR.

7 National Privacy Commission, Implementing Rules and Regulations of the Data Privacy At of 2012, available at https://privacy.gov.ph/implemening-rules-and-regulations-of-republic-act-no-10173-known-as-the-data-privacy-act-of-2012/

8 The definition of 'establishment' has been considered by the Court of Justice of the European Union under the Data Protection Directive 1995 in the case of C- 230/14 Weltimmo (see paras 28, 30 and 31) and C-131/12 Google Spain (see para 52).

9 Privacy International, 'Why should companies like Facebook commit to applying GDPR globaly?' Available at: https://privacyinternational.org/feature/1754/why-should-companies-facebook-commit-applying-gdpr-globally

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 3:

Data Protection Principles

Fair, lawful and transparent

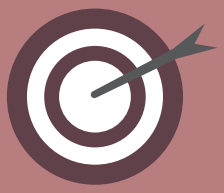
The processing of personal data should be lawful and fair and done in a transparent manner.

Purpose limitation

Personal data should be processed for a specified, explicit and legitimate purpose, stated at the point of collection, and further processing also compatible with this purpose.

Minimisation

The processing of personal data should be adequate, relevant and limited to necessity of the purpose for which it is being processed.



Accuracy

Personal data that is processed should be accurate, complete and measures should be taken to ensure it is up to date.

Storage Limitation

Personal data should only be retained for the period of time that is necessary for the purposes for which it was processed.

Integrity and Confidentiality

Appropriate measures must be taken to ensure security of data and systems, and to protect personal data from loss, unauthorised access, destruction, use, modification or disclosure.

Accountability

Those that process personal data must be accountable for demonstrating compliance with the above principles, their obligations, and facilitate and fulfil the exercise of these rights.

Data Protection Principles

Where a comprehensive data protection law exists, organisations, public or private, that collect and use your personal information have an obligation to handle this data according to data protection law. Derived from regional and international frameworks, a number of principles should be abided by when processing personal data.

Fair, Lawful, and Transparent

OECD: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

Convention 108: "Personal data undergoing processing shall be processed lawful" and "Personal data undergoing processing shall be processed … fairly and in a transparent manner" [Article 5 (3) and (4)(a)]

GDPR: "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject" [Article 5 (1)(a)]

Personal data must be processed in a lawful and fair manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. 'Fairness and transparency' are essential for ensuring that people's data is not used in ways they would not expect. 'Lawful' means that data must be processed in a way that respects of rule of law and that meets a legal ground for processing. A 'legal ground' is a limited justification for processing people's data set out in law (e.g. consent) - discussed in the below section on 'Lawful Grounds for Processing'.

Why does this principle matter?

It is crucial that the individual is clearly informed and aware of how their data is going to be processed, and by whom. If there is an intention to share the data of an individual with a third party but the data controller is not transparent about this fact and the data subject is not clearly informed, it is likely that their personal data was obtained unfairly, and the process will not be considered transparent.

For example, in Ireland, an insurance company contacted one of its customers to inform them about a new credit card, but it was unclear to the customer that it was not the insurance company who would be providing the new card, but that the data was instead transferred to bank to process – i.e. the bank was the data controller, but this had not been made clear to the individual in the communication that they received from their insurance company. It was therefore judged to have been unfairly processed.[1]

It is not enough to just be clear about what you are doing with people's data, but the lawful criteria included in this principle means that an entity must be justified in doing so by satisfying a legal ground.

Purpose Limitation

OECD: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

Convention 108: "Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes." [Article 5 (4)(b)]

GDPR: "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes." [Article 5 (1) (b)]

All personal data should be collected for a determined, specific, and legitimate purpose. Any further processing must not be incompatible with the purposes specified at the outset (i.e. the point of collection). This essentially means that it is not acceptable to state that you need a person's data for one purpose, and then use it for something else without notice or justification.

Technological developments (and the mass generation, collection, and analysis of data which accompany them) mean that these principles are ever more important. The purpose of processing and the proposed use of the data must be clearly defined and explained to the data subject. If the data is to be used for a purpose other than the original purpose, then the data subject should be adequately informed of this and a legal condition for this processing identified; this may necessitate obtaining further consent. It is particularly important that sensitive personal data is not processed for purposes other than those originally specified.

This is particularly relevant to big data and other data analysis processes. For example, the data broker industry thrives off the re-purposing of data:[2] they amass data from a vast array of sources, then compile, analyse, profile, and share insights with their clients. This means that a lot of data shared for one purpose is re-purposed in ways they might not expect, including targeted advertising.

Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, in accordance with the 'Purpose Limitation Principle'.

There are, however, two common exceptions to this principle: it is acceptable if done:

a) with the consent of the data subject
b) by the authority of law

While these are two widely recognised exceptions to the use limitation principles, they are often abused and misused. In the case of (a), consent must be valid; it must not be conditional, obtained through pre-ticked boxes, or have the details of these other purposes hidden in small print or legalese (inaccessible to the average data subject). In the case of (b), this has been used to allow for wide data-sharing arrangements by state bodies and institutions in the exercise of their functions, for example, using data provided for healthcare or education purposes for immigration purposes. Such blanket exemptions threaten to weaken the protection offered by data protection law, so it is crucial that any provisions providing for exceptions be narrowly constructed, so that the principle of purpose limitation is not made redundant and unenforceable when it comes to the State and its functions, and exchanges of information between state agencies and that there are limits on the reliance on consent, for example where there is an imbalance of power.

Furthermore, in relation to purpose limitation, the text of a law could provide for various purposes which should not be incompatible with this principle.

These could include, but are not restricted to:

- Archiving purposes in the public interest
- Scientific, statistical or historical purposes

It is essential that these purposes be restricted in their scope, and the above terms be further defined to provide clarity as to what each could entail.

Why does the purpose limitation principle matter?

If no clear limitations are established at the point of collection as to the uses of the data, there are concerns that the data could be used for other objectives over the data lifecycle, which could have detrimental effects on individuals and lead to abuse. There are an increasing number of cases in which the principle of purpose limitation is being undermined and bypassed. For example, Aadhaar, India's national biometric database, was originally established in 2009 with the aim of standardising government databases. However, over time, the project has become more ambitious and it is now being used for an array of purposes from school admissions to obtaining death certificates.[3] Eurodac, a biometric database established in 2000 to enable EU Member States to check whether an asylum seeker had previously applied for asylum in another European country or was receiving social benefits from another EU country, is now being used for a new purpose. The updated Eurodac Regulation, which came into force in July 2015, now allows for the "use of the Eurodac database of asylum-seekers' fingerprints for preventing, detecting and investigating terrorist offences and other serious crimes."[4]

Minimisation

OECD: "Personal data should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

Convention 108: "Personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed." [Article 5 (4) (c)]

GDPR: "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." [Article 5(1)(c)]

Data minimisation is a key concept in data protection, both from an individual's rights and an information security perspective. The law should clearly stipulate that only the data which is necessary and relevant for the purpose stated should be processed. Any exceptions to this must be very limited and clearly defined.

- **Necessity**: ensuring that the data collected is not intended to be more far-reaching than is necessary for the purposes for which the data will be used. The test should be that the least intrusive method is used to achieve a legitimate aim.

The "purpose test" – as the OECD has called it – "will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating." The concept of necessity also entails an assessment of whether the same aim could be achieved in a way that is less intrusive i.e. uses less data.[5]

- **Relevancy**: Any data processed must relevant to the purposes established.

Why does the data minimisation principle matter?

This principles requires that those processing data to consider what the minimum amount of data necessary to achieve the purpose would be. Processors should hold that and no more - it is not acceptable to collect extra data because it might be useful later on, or simply because no thought has been given to whether it is necessary in a specific scenario.

For example, it would be excessive to process precise and detailed location data for connected cars for a purpose involving technical maintenance or model optimisation.[6]

The principle of data minimisation is even more integral in the age of big data, where advancement in technology has radically improved analytical techniques for searching, aggregating, and cross-referencing large data sets in order to develop intelligence and insights.[7] With the promise and hope that having more data will allow for accurate insights into human behaviour, there is an interest and sustained drive to accumulate vast amounts of data. There is an urgent need to challenge this narrative and ensure that only data that is necessary and relevant for a specific purpose should be processed.

Accuracy

OECD: "Personal data should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

Convention 108: "Personal data undergoing processing shall be accurate and, where necessary, kept up to date." [Article 5 (4) (d)]

GDPR: "Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." [Article 5(1)(d)]

Personal data must be accurate throughout processing and every reasonable step must be taken to ensure this. This includes the following elements:

- **Accuracy**: All data processed must be accurate throughout the data lifecycle;
- **Complete**: Any category of data must be complete to the extent possible that the omission of relevant data may not lead to the inference of different information to the information that could be obtained if the data were complete;
- **Up-to-date**: Any data that is retained and may be further processed in accordance with the provisions provided for in the data protection law must be kept up-to-date; and
- **Limited**: Personal data should only be processed (and retained) for the period of time it is required for the purpose for which it was collected and stored.

The above elements reaffirm the rights of data subjects to access their personal data, and to correct incomplete, inaccurate, or outdated data which should be provided for in a data protection law.

Why does the accuracy principle matter?

Increasingly, decision- and policy-making processes rely on data. However, there is a high risk that if the data is not accurate and up-to-date, then the outcome of the decision-making process will also be inaccurate. In the most serious scenarios, this could lead to a decision that an individual is not granted access to public services, or to welfare programmes, or given a loan. For example, there have been incidences of individuals wrongly denied a loan or re-mortgage on their house because the company in charge of reviewing their credit score had inaccurate information which brought down their rating from 'Excellent' to 'Poor', or because inaccurate information was registered by banking institutions which made an individual an undesirable customer.[8]

Storage Limitation

Convention 108: "Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored" [Article 5(e)]"

GDPR: "Personal data undergoing processing shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject. ('storage limitation')" [Article 5 (1) (e)]

Personal data should only be retained for the period of time that the data is required for the purpose for which it was originally collected and stored. This will strengthen and clarify the obligation to delete data at the end of processing, which should be included in another provision.

The law should clearly stipulate that data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be very limited and clearly defined.

Just because the data controller might come across another use of the data does not justify blanket or indefinite retention. How long it is necessary to store data will be context-specific, however, this should be guided by other legislative obligations and regulatory guidance. For individuals to be fairly informed about the processing of their data, they must be informed how long their data will be retained, it is therefore imperative that legislation incentivises data controllers to implement the data minimisation principle by minimising the collection of personal data, and not storing it longer than necessary.

Data controllers should establish retention schedules specifying the retention periods for all the data that they hold. These should be kept under regular review. This is separate to the deletion of personal data on the request of the data subject, which must also be provided for in the legislation. After the necessary time period, personal data should be securely deleted. If data is to be stored beyond the retention period in an anonymised (and not pseudonymised) form, the privacy implications and consequences for the data subjects must be carefully considered.

Why does the storage limitation principle matter?

Even if data has been processed fairly, lawfully, in a transparent manner, and with respect to the principles of purpose limitation, minimisation and accuracy, it is essential to ensure that the data is not stored for longer than required and necessary for the purpose for which it was collected.

Any interference with the right to privacy and data protection requires to be necessary and proportionate. Blanket data retention completely fails to respect this – as confirmed in 2014, when the European Court of Justice struck down the Data Retention Directive, calling mandatory data retention, "an interference with the fundamental rights of practically the entire European population...without such an interference being precisely circumscribed by provisions to ensure that is actually limited to what is strictly necessary". This decision represented a strong authoritative recognition of the safeguards that must be in place to protect our right to privacy.[9]

Indefinite data retention is not only an infringement of the rights of an individual but a risk for those processing it. Failure to limit the period for which data is stored increases security risks and raises concerns that it could be used for new purposes merely because it is still available and accessible. There are risks that, if outdated, it could lead to poor decision-making processes which could have severe implications.

In the age of widespread, unregulated state and corporate surveillance,[10] it is essential that strict limitations are placed on data retention to mitigate possible unlawful interferences with the right to privacy.

Integrity and Confidentiality

OECD: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

Convention 108: "Each Party shall provide that the controller, and, where applicable the processor, take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data." [Article 7 (1)]

GPDR: "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" [Article 5 (1) (f)])

Personal data, at rest and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data.

Security safeguards could include:

- Physical measures, i.e. locked doors and identification cards, for instance;
- Organisational measures, i.e. access controls;
- Informational measures, i.e. enciphering (converting text into a coded form), and threat-monitoring; and
- Technical measures, i.e. encryption, pseudonymisation, anonymisation.

Other organisational measures include regular testing of the adequacy of these measures, implementation of data protection and information security policies, training, and adherence to approved codes of conduct.

Why does the security safeguards principle matter?

If security measures are not taken to protect data, and ensure the security and safety of the infrastructure, data is left vulnerable to threats and is at risk of breach and unlawful access. There have been multiple examples of data breaches as a result of weak security.

For example, in March 2016, the personal information of over 55 million Filipino voters were leaked following a breach on the Commission on Elections' (COMELEC's) database. In September 2016, the National Privacy Commission concluded that there had been a security breach that provided access to the COMELEC database that contained both personal and sensitive data, and other information that may be used to enable identity fraud. The personal data included in the compromised database contained passport information, tax identification numbers, names of firearm owners and information about their firearms, and email addresses. A preliminary report identified that one of the indicators of negligence on behalf of COMELEC was vulnerabilities in their website, and failure to monitor regularly for security breaches.[11]

In July 2016, due to security failures, a database of the Municipality of São Paulo, Brazil, was published exposing personal data of an estimated 650,000 patients and public agents from the public health system (SUS). The data included addresses, phone numbers, and even medical data. Details of pregnancy stages and cases of abortion were also exposed.[12]

Accountability

OECD: "A data controller should be accountable for complying with measures which give effect to the principles stated above"

Convention 108: "Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention." [Article 10 (1)]

GDPR: "The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1"[13] ('accountability') [Article 5 (2)]

An entity which processes personal data, in their capacity as data controllers or processors, should be accountable for complying with standards, and taking measure which give effect to the provisions provided for in a data protection law. Those with responsibility for data processing must be able to demonstrate how they comply with data protection legislation, including the principles, their obligations, and the rights of individuals.

Why does the accountability principle matter?

The accountability principle is key to an effective data protection framework. It brings together all the other principles and puts the onus on those processing people's data (whether a company or a public authority) to be responsible for and to demonstrate compliance with their obligations. In practice, this means that those processing personal data should be more open and proactive about the way they handle data in compliance with their obligations. They must be able to explain, show, and prove that they respect people's privacy - both to regulators and individuals.

The importance of the accountability principle is clearest when considering contexts in which there are no accountability mechanisms in place – i.e. where there is no structure to report breaches of the law.

For example, in South Africa, The Protection of Personal Information (PoPI) Act was adopted in 2013, providing for the establishment of an Information Regulators, though this body was not put in place until April 2017. At present, data breaches in South Africa often go unreported: in 2015, it was reported

that only five data breaches were registered in South Africa.[14] This is expected to change significantly as PoPI comes into force, as responsible parties will be required by law to disclose information about data breaches if they occur.

Accountability mechanisms play an important role in investigating breaches and holding entities subject to the law to account. In 2017, following revelations of a major leak of data from taxi hire app Uber in 2016, the Mexican National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) asked Uber for information on the number of "Mexican users, drivers and employees" who had been affected.[15] The institute also asked Uber for information on the measures the company is taking to mitigate damage and protect clients' information.

References

1 Data Protection Commission (Ireland), 'Case Study 1/01', available at: https://www.dataprotection.ie/docs/Case-Study-1-01-Bank-and-Insurance-Company/121.htm

2 Privacy International, 'How do companies get our data?' available at: https://www.privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

3 The Centre for Internet and Society, 'Aadhaar Act and its Non-compliance with Data Protection Law in India', 14 April 2016, available at: https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india; and Usha Ramanathan, 'Aadhaar: from compiling a government database to creating a surveillance society', Hindustan Times, January 2018, available at: https://www.hindustantimes.com/opinion/aadhaar-from-compiling-a-govt-database-to-creating-a-surveillance-society/story-Jj36c6tVyHJMjOhCI8vnBN.html

4 Costica Dumbrava, 'European Information Systems In The Area Of Justice And Home Affairs: An Overview', European Parliamentary Research Service Blog, 15 May 2017, available at: https://epthinktank.eu/2017/05/15/european-information-systems-in-the-area-of-justice-and-home-affairs-an-overview/

5 For example, see CJEU case of Osterreichischer Rundfunk C-138/01 2003

6 Commission National Informatique & Libertes, Compliance Package: Connected Vehicles and Personal Data, available (PDF) at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

7 Privacy International, Big Data - Explainer, available at: https://privacyinternational.org/explainer/1310/big-data

8 Maria LaMagna,' The reason your loan application is rejected may have nothing to do with your credit score', MarketWatch', 29 March 2017, available at: https://www.marketwatch.com/story/the-reason-your-loan-application-is-rejected-may-have-nothing-to-do-with-your-credit-score-2017-03-29; Anna Tims, 'Equifax mistake with my credit score nearly lost me a mortgage', The Guardian, 14 February 2017, available at: https://www.theguardian.com/money/2017/feb/14/credit-rating-remortgage-equifax-experian-callcredit; and Anna Tims, 'How credit score agencies have the power to make or break lives', The Guardian, 17 July 2017, available at: https://www.theguardian.com/money/2017/jul/17/credit-score-angencies-break-lives-lenders-no-mortgage

9 Court of Justice of the European Union, 'The Court of Justice declares the Data Retention Directive to be invalid', Curia, available (PDF) at https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

10 Privacy International, Contesting Surveillance, available at https://www.privacyinternational.org/programmes/contesting-surveillance; and Privacy International, Challenging Data Exploitation, available at https://www.privacyinternational.org/programmes/challenging-data-exploitation

11 Foundation for Media Alternatives, 'National Privacy Commission to issue findings on Comelec breach' available at: http://www.fma.ph/?p=399

12 Raphael Hernandes, 'Gestao Haddad expoe na internet dados de pacientes de rede publica', Folha de S. Paulo, 6 July 2016, available (Portuguese) at: http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml

13 Paragraph 1 of Article 5 of the GDPR outlines the principles relating to processing of personal data.

14 Duncan Alfreds, 'SA fails to make data breaches public – expert', Fin24, 26 February 2016, available at https://www.fin24.com/Tech/Cyber-Security/sa-fails-to-make-data-breaches-public-expert-20160226

15 R3D: Red en Defensa de los Derechos Digitales, 'INAI pide a Uber revelar si robo masivo de datos afectó a usuarios mexicanos', available (Spanish) at: https://r3d.mx/2017/12/01/inai-pide-a-uber-revelar-si-robo-masivo-de-datos-afecto-a-usuarios-mexicanos/#more-4034

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 4:

Rights of Data Subjects

Rights of Data Subjects

Right to Information

Individuals must be informed about how their personal data is being processed both where they have provided this directly to a data controller and where the controller has obtained it from another source, i.e. a third party.

Right to Access

Individuals should be informed when their personal data is being collected and they must be able to obtain (request and be given) information about the processing of their personal data.

Right to Object

Individuals should have the right to object to their personal data being processed.

Rights to Rectify, Block and Erasure

Individuals should have the right to rectify, block, and to request the erasure of data processed about them to ensure that such data is accurate, complete, and kept up-to-date.

Rights Related to Profiling and Automated Decision Making

All rights contained in the law should apply to profiling and automated decision making and include the right to request human intervention or to challenge a decision.

Right to Data Portability

Individuals should have the right to obtain all of their personal data from a data controller in a universally machine-readable format or for that data to be ported to another service should they request it.

Right to an Effective Remedy

Individuals should have the right to an effective judicial remedy where they consider that their personal data was not processed in compliance with the law.

Right to Compensation

A person whose rights have been found to be violated has a right to compensation for the damage – material or non-material – suffered.

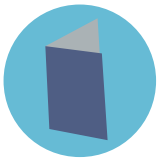
Rights of Data Subjects

A central component of any data protection law is the provision of the rights of individuals, who are often referred to as the data subjects.

These rights should appear early in the law, as they should be seen as applying throughout, underpinning all provisions in the law. These rights impose positive obligations on data controllers and should be enforceable before independent data protection authority and courts.

At minimum, these should include:

- Right to information
- Right to access
- Rights to rectify, block and erasure
- Right to object
- Right to data portability
- Rights related to profiling
- Rights related to automated decision making
- Right to an effective remedy
- Right to compensation and liability.



Right to Information

Individuals must be provided with information about how their personal data is being processed, both where they have provided this directly to a controller and where the controller has obtained it from another source.

Individuals should be provided with at least the following information:

- information as to the identity of the controller (and contact details)
- the purposes of the processing
- the legal basis for processing
- the categories of personal data
- the recipients of the personal data
- whether the controller intends to transfer personal data to a third country and the level of protection provided
- the period for which the personal data will be stored
- the existence of the rights of the data subject
- the right to lodge a complaint with the supervisory authority
- the existence of profiling, including the legal basis,

the significance and the envisaged consequence of such processing for the data subject
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject
- the source of the personal data (if not obtained from the data subject)
- whether providing the data is obligatory or voluntary
- the consequences of failing to provide the data

Taking informed decisions and knowing your rights

In order to be able to make an informed decision about whether to use a system or a service and share their data, and so that they can exercise their rights, individuals must be informed when, why, and how their data is being processed.

Functionalities and technicalities of services mean that, on a technical level, a data controller could be processing data without the individual even knowing. For example, some applications are processing vast amounts of data about users, but the user is given little or no information about this, and when they are given information, it is not comprehensible to the average user. In the case of application NaMo, permissions relating to data were not compulsory, and could only be found in the 'Read More' section of the app. Consequently, users were not informed what data the application was processing when downloading the app.[1]

Right to Access

To enable a data subject to exercise and enjoy their rights, and for their enforcement to be effective, the data subject must be able to obtain (i.e. to request and be given) information about the collection, storage, or use of their personal data. The information should include, at least, confirmation of whether a controller processes data about them, the purpose of processing, the legal basis for processing, where the data came from, who it has been/might be shared with, how long it will be stored for, and information about how their data is being used for profiling and automated decision-making. This information should be accompanied by a copy of the requested data.

It is not sufficient merely for the right to be upheld. The law should provide minimum requirements, including for the process of obtaining data relating to those requirements. These include requirements on:

- Timeframe: this should be within a reasonable and stated time.
- Cost: individuals should bear no cost for obtaining information about processing and a copy of their personal data.
- Format: the information provided to the data subject should be in a form that is readily intelligible to them and does not require them to have any particular expertise or knowledge in order to comprehend the information they are provided with.
- Explanation and appeal: if the request is denied, the data subject has a right to be given reasons why, and to be able to challenge such denial. Furthermore, if their challenge is successful they must have the right to have the data erased, rectified, completed or amended.
- Clarity: if there are to be any exemptions to this right these should be clearly set out in law and their application explained to the data subject.

Access rights are an important tool for individuals, journalists, and civil society to investigate, review, and expose how personal data is being processed. A clear and prescriptive law is the starting point for the enjoyment of these rights in practice.

Right to access in practice

The right of access is an essential right for individuals to understand what data is being processed about them and how. Accessing their data enables then people to check whether their data is being processed in line with the law and their expectations, whether its accurate and whether they want to take further action, such as exercising their right to object. This can help them uncover why decisions were made and also expose abusive data practices. This could be, for example, in the context of employment, healthcare, education, financial services or online services. At PI we've made access requests to understand how data is processed on cars[2] and how companies such as data brokers use our data in a largely hidden data ecosystem.[3] Access requests have been used to seek to find out about the use of data in elections,[4] dating apps[5] and telecommunication providers,[6] to name a few.

Openness principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle

13. An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial.
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.[7]

Rights to Rectify, Block and Erasure

A data subject has the right to rectify and block (restrict) data processed about themselves to ensure the data is accurate, complete and kept up-to-date and that it is not used to make decisions about them when the accuracy is contested.

An individual should have the right to demand that the data controller correct, update, or modify the data if it is inaccurate, erroneous, misleading, or incomplete.

Individuals also have the right to 'block' or suppress processing of personal data in particular circumstances. Personal data can then be stored but not further processed until the issue is resolved.

Another right included within many data protection frameworks, such as the GDPR, Nigeria, and South Africa, is the right to erasure. A right to erasure permits data subjects in certain circumstances (i.e. when there is no lawful basis for processing) to request that the data controller erase his/hertheir personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. It is essential that provision is made to ensure among other safeguards, that when processing the request, the data controller will considers the public interest of the data remaining available. It is essential that any such right clearly provides safeguards and in particular exemptions for freedom of expression. The construction of this right and how it will play out in the national context must be considered very carefully to ensure that it is not open to abuse.

Rectifying data and the difference it can make

In light of the data-driven decision-making processes being adopted by governments and industry alike, and the automated nature of data processing (where an individual may not know their personal data is being collected), the need to ensure that the data being processed is accurate more important than ever.

If inaccurate medical data is processed, it could lead to individuals not receiving the medical assistance they need. A mistake in a postal address held by a consumer credit reporting agency could lead to an individual's credit score being poorly (albeit incorrectly) rated resulting in their mortgage application being turned down, as occurred with Equifax Inc.[8]

The UN Human Rights Committee, in interpreting the scope of obligations of state parties to the International Covenant on Civil and Political Rights (of which India is a party since 1979), noted its General Comment No 16 on Article 17 of the ICCPR, back in 1989, that:

> **"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."**

Right to Object

An individual has the right to object to their data being processed at any point. If the individual objects, the onus must be on the data controller to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Certain rights to object should be absolute, such as in relation to direct marketing.

Implementing right to object: opt-out by default

When it comes to direct marketing, opt-out was previously the standard approach but in Asian countries new restrictions have been put in place: Hong Kong and South Korea have enacted the tougher opt-in requirements, with severe financial penalties for breaches; all of the others (except Singapore and the Philippines) have some direct marketing restrictions.[9]

Right to Data Portability

Every individual should have the right to request that personal data about themselves that is processed by the data controller be made available to them in a universally machine-readable format, and to have it transmitted to another service with the specific consent of that individual. This right is a step towards ensuring that the data subject is placed in a central position and has a full power over his or her personal data.

Rights Related to Profiling and Automated Decision Making

A data protection law should provide effective protection and rights in relation to both profiling and automated decision-making. This should include all of the above rights; additional rights and guarantees apply exclusively to both profiling and automated decision making to address specific concerns related to these ways of processing personal data.

These rights do not need to be dealt with together as this can lead to unnecessary confusion. However, it is important that both are covered in a data protection framework.

Profiling

Profiling occurs in a range of contexts and for a variety of purposes; from targeted advertising and healthcare screenings to predictive policing. Profiling as a process recognises the fact that data can be derived, inferred and predicted from other data. This can be used to score, rank and evaluate and assess people, and to make and inform decisions about individuals that may or may not be automated. Through profiling, sensitive data (i.e. data revealing particularly sensitive traits of an individual, such as race, political opinions, religious or philosophical beliefs; biometric and health data, etc.) can be inferred from other non-sensitive data.

Profiling, just as any form of data processing also needs a legal basis.
The law should require that organisations who profile are transparent about it and individuals must be informed about its existence. Individuals must also be informed of inferences about sensitive preferences and characteristics, including when derived from data which is not per se sensitive. Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their rights, including to access, rectification and deletion. Individual's rights need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data.

Profiling in practice: targeted online advertising

Non-consumer facing data companies collect data from different public and private sources[10], both on behalf of clients and for their own purposes. They carry out profiling by compiling, analysing and evaluating information about individuals, placing them into certain categories and segments.

Profiles feed into targeted online advertising which can be invasive[11] and manipulative, and also has the potential to lead to the exclusion or discrimination of individuals. A 2015 study by Carnegie Mellon University researchers, for instance, found that Google's online advertising system showed an ad for high-income jobs to men much more often than it showed the ad to women.[12] The study suggests that such discrimination could either be the result of advertisers placing inappropriate bids, or an unexpected outcome of unpredictable large-scale machine learning. Intentional or not - such discrimination is an inherent risk of targeted advertising and impossible for individuals to detect.

Automated decision-making

As a result of advancements and innovation in technology and the significant increase in data generated, there are new ways of processing personal data. Data is increasingly playing an important role in decision-making.[13]

This a growing reliance on automated decision-making which is making it difficult to interpret or audit decision-making processes, yet can still produce decisions that are inaccurate, unfair or discriminatory.

> **Automated-decision making in practice**
>
> An example is the use of automated risk scores in the criminal justice system. Proprietary software, such as the COMPAS risk assessment system, that has been sanctioned by the Wisconsin Supreme Court in 2016, calculates a score that predicts the likelihood of an individual committing a future crime.[14] Even though the final decision is formally made by a judge, the automated decision made by a programme can be decisive, especially if judges rely on it exclusively or have not received warnings about the risks of doing so, including that the software potentially producing inaccurate, discriminatory or unfair decisions.

Because of the heightened risks to human rights and freedoms and issues such as fairness, transparency and accountability, data protection frameworks may impose restrictions and safeguards on the ways in which data can be used to make decisions. These safeguards should a right not to be subject to certain automated decisions as this is important where these decisions are consequential for individuals, and in particular where they affect their rights.

Individuals should have a right not be subject to purely automated decision-making. It is important that the law frames this right as a clear prohibition of automated decision-making which protects individuals by default. The law may provide for certain exemptions, i.e. as when it is based on a law (e.g. fraud prevention), or when the individual has given their explicit consent. However, any such exemptions must be limited, as well as and clearly and narrowly defined.

The law must be clear as to what kinds of decisions this right applies to. For example, in the GDPR, Article 22 provides rights in relation to solely automated decisions which have legal or other significant effects. The meaning of these concepts is not crystal clear on the face of the legislation and has required guidance – which makes clear that a decision with fabricated human involvement is also subject to safeguards and that examples of legal or other significant effects include: refusal to grant child or housing benefit; refusal of entry at the border; being subjected to increased security measures or surveillance; or automatically disconnection of from their mobile phone service for breach of contract; automatic refusal of an online credit application, ‘e-recruiting’ practices without any human intervention.

Right to human intervention

Even where exemptions allow for automated-decision making, an individual should have the right to obtain human intervention.

Automated decision-making without human intervention should be subject to very strict limitations. This is particularly important in the law enforcement sector, as a potential miscarriage of justice can scar an individual and impact their wellbeing for life.

As noted above, with reference to the guidelines on automated decision-making and profiling by the Working Party 29 (i.e. the body representing all national data protection authorities in the EU, including the ICO which led on the consultation of this document):

> **To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.[15]**

Right to an Effective Remedy

The law must include the right of an individual to an effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law.

A data subject must have the right to submit a complaint to the independent supervisory authority. This reaffirms the need for the independent supervisory authority to have the power to receive complaints from data subjects, investigate them, and sanction the violator within their own scope of powers - or refer the case to a court. The law should also provide for the data subject to take action against a supervisory authority where they have failed to deal with their complaint.
As well as the right to complain to a supervisory authority, individuals should also have access to an effective judicial remedy via the courts. Individuals should be empowered to take action themselves, as well as instructing others (including NGOs) to take action on their behalf.

In addition, an important and effective mechanism for holding those that fail to comply with data protection law to account is collective redress. Often individuals will not have the resources to investigate and uncover non-compliance, draft complaints, and take further legal action. The cost and complexity of the process

can render their redress mechanisms inaccessible and ineffective in practice. Therefore, a collective redress mechanism should allow NGOs with knowledge of data protection to pursue data protection infringements on their own initiative.[16] Specific provision for NGOs to take action is particularly important in the context of legal frameworks where there might be no other mechanism for collective redress in the field of data protection (i.e. injunctive remedies).

Due to power imbalances and information asymmetries between individuals and those controlling their personal data, data subjects remain as unlikely to pursue cases under the new laws in the future as they were in the past, notwithstanding enhanced enforcement rights. Allowing collective redress would be an effective means to strengthen enforcement.

> **An example of access to effective remedy in action**
>
> The German Consumer Federation took Facebook to court over a number of its breaches of current German Data Protection Legislation; the Court judgement of February 2018 upheld the majority of the consumer organisation's claims, including unlawful terms and conditions and consent provisions in its default privacy settings.[17]

Right to Compensation and Liability

A person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress).

This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority.

Exceptions

It is very common that there would be a provision providing for exceptions to compliance with certain principles, obligations, and rights. Often exceptions will relate to the processing of personal data by public authorities - in particular security and intelligence agencies.

It is essential to ensure that, where it provides for such exceptions, the law also provides in-depth details on the specific circumstances in which the rights of data subjects can be limited. These provisions should be limited, necessary and proportionate, and be clear and accessible to the data subject. Moreover, these should not be blanket exceptions but must only pertain to certain rights in very specific and limited situations and be clearly set out by the law.

References

1 Krishn Kaushik, 'Narendra Modi App asks for sweeping access: Camera, audio among 22 inputs', The Indian Express, 26 March 2016, available at http://indianexpress.com/article/india/namo-app-asks-for-sweeping-access-camera-audio-among-22-inputs-facebook-data-leak-5111353/

2 Privacy International, Connected Cars: What Happens To Our Data On Rental Cars?, 6 December 2018, available at: https://privacyinternational.org/report/987/connected-cars-what-happens-our-data-rental-cars

3 Privacy International, Uncovering the Hidden Data Ecosystem, available at: https://privacyinternational.org/campaigns/uncovering-hidden-data-ecosystem

4 Jeremy B White, 'Cambridge Analytica ordered to turn over man's data or face prosecution', The Independent, 5 May 2018, available at: https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-ordered-ico-personal-data-david-carroll-a8338156.html

5 Judith Duportail, 'I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets', The Guardian, 26 September 2017, available at: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

6 Hilts, A., Parsons, C., and Crete-Nishihata, M., Approaching Access - A look at consumer personal data requests in Canada, CitizenLab, 12 February 2018, available at: https://citizenlab.ca/2018/02/approaching-access-look-consumer-personal-data-requests-canada/

7 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

8 Tims, Equifax Mistake, op. cit.

9 Greenleaf, Asian Data Privacy Laws (OUP, 2014), p. 493

10 Privacy International, How Do Data Companies Get our Data?, 25 May 2018, available at: https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

11 For example, targeting of insecure young people, See: Sam Levin, 'Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'', The Guardian, 1 May 2017, available at: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

12 Datta, A., Tschantz, M. C., & Datta, A. Automated Experiments on Ad Privacy Settings, Proceedings on Privacy Enhancing Technologies, 2015(1), 92–112. Available at https://doi.org/10.1515/popets-2015-0007

13 Privacy International, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR', 2017. Available at: https://www.privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

14 Danielle Citron, '(Un)Fairness of Risk Scores in Criminal Sentencing', Forbes, 13 July 2016, available at https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/#146a7f514ad2

15 Article 29 Working Party on Data Protection, Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

16 For reference in a UK/EU context, see: Anna Fielder, 'Why we need collective redress for data protection', Privacy International Medium, 9 January 2018, available at https://medium.com/@privacyint/why-we-need-collective-redress-for-data-protection-863c6640689c

17 English press release available at: https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 5:

Grounds for Processing of Personal Data

Grounds for Processing of Personal Data

A data controller or processor must identify the legal basis by which their processing of personal data is permitted.

The grounds for processing personal data should be limited and clearly spelled out in law (i.e. there should not be vague, broad grounds, or open list of possible grounds for processing.) Too often, however, laws provide for many grounds.

Grounds for Processing of Personal Data

- consent of the data subject
- ensuring the necessity of the processing for the performance of a contract with the data subject or to take steps to enter into a contract
- for compliance with a legal obligation
- to protect the vital interests of a data subject or another person
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Some of these are discussed below in more detail.

Consent

Consent is a core principle of data protection which allows the data subject to be in control of when their personal data is processed: it relates to the exercise of fundamental rights of autonomy and self-determination.

Consent must be freely given, specific, informed, and unambiguous, and can be a written statement, including by electronic means. It should be explicit and require an active process for the individual, rather than a passive opt-out process: as such, it requires positive affirmative action. The entity processing the data must be able to demonstrate they sought and received consent.

Consent is not the only legal ground for processing. In fact, in many situations where there is a power imbalance between the individual and the processor (e.g. between employee and employer), consent cannot be freely given and therefore another legal ground must justify the processing of the personal data (e.g. performance of a contract.)

Explicit, freely given and unambiguous

The definition of consent should reflect individual's free and informed choice. For example, the GDPR contains the following definition:

> **'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.**

Exemptions for Public Institutions

In some jurisdictions, notice and consent are not required when the processing is undertaken by a public institution during the exercise of its legal functions. This is the case in Colombia in Article 10 (a) of Law 1581 of 2012, which regulates the processing and management of personal information.

It is crucial that such processing is subject to suitable and specific measures to protect the rights and freedoms of individuals.

Implied consent

Some texts may include the concept of implied consent. This was the case in the draft bill proposed for the amendment of the data protection law in Argentina. Privacy International does not believe that 'implied' consent meets the standards of specific, freely given, informed and unambiguous consent.

The Article 29 Working Group (the Group of European data protection authorities) has studied the question of consent, and in particular implied consent, and concluded that implied consent would "not be apt to the GDPR standard of consent."[1]

Particular attention must be given to such a provision to ensure there are clear guidance and conditions as to the contexts in which implied consent would be sufficient.

Withdrawing consent

Data subjects should have the right to withdraw their consent at any time. Prior to collecting data, a data controller should be obliged to inform the data subject (at a point prior to obtaining consent) of their right to withdraw consent. This provision should include that any revocation of consent should lead to deletion of the personal data. Consent should be as easy to withdraw as it is to provide. The data controller should take positive action to confirm with the individual that their request has been processed, their consent withdrawn, and their data deleted.

Reliance on consent should not negate the obligation on data controllers to comply with the data protection principles including transparency, fairness, purpose limitation, and data minimisation. Even when relying on consent, data controllers should carefully consider (for example through a data protection impact assessment) any prejudice to the rights of individuals as a result of the processing, and take steps to mitigate these.

Public Interest

Another legal ground which is often recognised in data protection laws is the need for processing of personal data if the controller undertakes it in the public interest.

A key consideration here is that data protection law may not define what constitutes 'public interest' and will instead defer to those processing the data or the data protection authority to make that determination. The lack of definition, and clarity around what constitutes 'public interest' and its often-broad interpretation, raises concern that it can act as a loophole.
A public interest ground should be clearly defined to avoid abuse. For example, it should be possible to list the specific public interest grounds (e.g. administration of justice) and ensure that such a list is clear and exhaustive.

If there is to be a condition which permits processing of data in emergency situations, this should be carefully thought through and defined. All grounds for processing should be subject to other safeguards to protect the rights and interests of the data subject, including fairness, transparency and a data protection impact assessment which clearly takes into account any prejudice or adverse effect on individuals.

Therefore, recommendations for the data protection authority could include:

- Mapping legislation which include 'public interest' provisions to clarify what these could be
- Requesting that further guidance and a 'public interest' test be developed by the independent supervisory authority
- Requiring public authorities to state clearly what they consider the public interest to be
- If it is to be applied to allow for the processing of sensitive personal data, the independent supervisory authority must define in advance the high threshold of 'public interest' that needs to be met before sensitive personal data can be processed without consent or another legal basis

Legitimate Interest

Often data protection frameworks, will provide that where a legitimate interest can be demonstrated by the data controller, it may constitute a legal basis for data processing. Given the wide scope of the term legitimate interest it is essential that this condition is qualified. For example, the data controller must also demonstrate that: the processing is necessary and proportionate to the legitimate interest pursued and, it does not override the rights of the data subject.

This condition can be interpreted widely and is open to abuse. Its inclusion in legislation should be avoided if possible.

If this provision is included and there is any doubt in the balancing exercise that there is prejudice to the individual, then the presumption should be that the processing should not go ahead. Furthermore, it is imperative that data controllers provide clear notice to the individuals of the specific legitimate interest they are relying on (i.e. they cannot simply rely on generic or vague legitimate interest), and allow for assessment of prejudice to individuals on a case-by-case basis, including an opt-in mechanism.

Not all legal grounds for processing are available to all controllers. For example, the ability to resort to the justification of legitimate interest has been limited to public authorities under the GDPR. This means that public authorities cannot rely on this justification when processing is carried out in the course of the performance of their duties, but as a public authority they must identify the public interest and the relevant public task/statutory function.

Processing of Sensitive Personal Data

When processing sensitive personal data, further conditions must be met. The situations in which the processing of sensitive personal data is permitted should be limited. Where consent is to be relied upon to justify the processing of sensitive personal data, it is extremely important that it is explicit and meets all the consent requirements set out above (i.e. informed, free, specific).

To strengthen the principle of purpose limitation (provided for elsewhere in the law), the provision on sensitive personal data should reaffirm that sensitive personal data cannot be further processed for other purposes or by parties other than those identified in the law.

It is also important that the higher protections extend to data that reveals sensitive personal data, through profiling and the use of proxy information, it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data.

Conditions for processing sensitive personal data must be limited, and care should be taken where conditions are proposed such as 'where the data is manifestly made public by the data subject' (Article 9 of the GDPR). Such an approach raises questions: what does 'made public' mean? How can it be verified that it was made public by an individual, and importantly if an individual has made data public, does that mean that data can be used by anyone for any purpose?

This is particularly relevant in the light of recent developments: the evolution of the open data movement and public transparency laws have meant that there are an increasing number of databases and other registries (i.e. property registries, tax registries, or electoral databases) which hold personal data. The fact that these have been made public (for reasons of public interest, transparency, and accountability) does not mean that the data they hold should be permitted to be used for other purposes than those defined at the point of collection.

Furthermore, Privacy International has ongoing concerns over the use of social media intelligence (SOCMINT) as a technique by law enforcement and other security agencies, which is spreading worldwide. They argue that the use of this data, without being subject to any regulation, judicial authorisation, or independent oversight, is lawful as it does not interfere with the right to privacy, relying only on so-called "publicly available" data. We reject this argument. There are clear and serious privacy implications of processing 'publicly available' data on social networking platforms. The fact that data is publicly available does not justify unregulated and unchecked collection, retention, analysis, or other processing.[2]

Processing of personal data for scientific, historical, or statistical purposes

It is sometimes included within data protection frameworks that the processing of personal data for data for scientific, historical, or statistical purposes could be a ground for processing data.

In order to avoid abuse and wide interpretation of this ground:

- There is a need for clarity on what the statistical and scientific purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data controller or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data subject should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

Processing of personal data and freedom of expression and to information

A state must take the necessary measures to reconcile the right to protection of personal data with the right to freedom of expression and information. This can include processing for journalistic and human rights purposes, and the purposes of academic, artistic or literary expression. In having to do balance these two rights, there may be exemptions and derogations from the obligations and the rights of data subjects.

For journalism purposes, an exemption might apply to the extent that it is necessary for 1) protection of the right to exercise the fundamental right to freedom of expression and opinion for journalistic purposes and 2) the protection of sources. In addition, we would suggest that any such provision be expanded to include other legitimate exercises of freedom of expression, such as investigations carried out by independent non-governmental organisations.

References

1 Article 29 Working Party, Guidelines on consent under Regulation 2016/769, adopted on 28 November 2017, as last revised and adopted on 10 April 2018, pp. 30. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

2 For more information, see Privacy International's Explainer, available at: https://privacyinternational.org/explainer/55/social-media-intelligence

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 6:

Obligations of Data Controllers and Processors

Compliance and Accountability

Data controllers and processors should demonstrate how they comply with their respective data protection obligations.

Q: Does the law explicitly require that data controllers and processors demonstrate compliance? ☐

Recording Processing Activities

Data controllers and processors should be obliged to keep written records of their processing activities.

Q: Does the law:

- provide for this obligation? ☐
- specify the minimum information that must be recorded? ☐

Such as

- the name and contact details of the controller(s) and processor(s) ☐
- the purposes of the processing ☐
- the legal basis for processing ☐
- a description of the categories of data subjects and of the categories of personal data ☐
- the third-parties to whom the personal data have been or will be disclosed ☐
- the categories of third-parties to whom the personal data have been or will be transferred, including details of safeguards adopted ☐
- the envisaged time limits for erasure of the different categories of data ☐
- a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data ☐

Safeguarding Security, Integrity and Confidentiality

The data controller and the data processor must have the duty and responsibility to safeguard the security of data and the infrastructure.

Q: Does the law:

- provide for this obligation? ☐
- clearly outline the types of security and organisational measures which data controllers and processors should take to protect the integrity and security of the data? ☐

Suggested obligations could include but are not limited:

- the pseudonymisation of personal data
- the encryption of personal data
- a guarantee of ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly monitoring, evaluating and auditing effectiveness of safeguards

Adopting data protection by design and by default

Data protection should be embedded into systems, projects and services from the beginning to ensure that by design and default they implement the data protection principles and safeguard individual rights.

Q: Does the law oblige at the time of determination and during processing:

- 'Data protection by design' which requires implementing appropriate technical and organisational measures which are designed to effectively implement data protection principles. ☐
- 'Data protection by default' which requires implementing appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. ☐

Impact assessments

Data controllers and the data processors should undertake an impact assessment to be conducted prior to processing personal data.

Q: Does the law:

- provide for this obligation? ☐
- outline what must be assessed prior to processing personal data? ☐

An impact assessment requires at minimum assessment of:

- the necessity and proportionality of the processing,
- the risks to individuals and,
- how these are to be addressed.

Data Protection Officers

The data controller and processors should designate responsibilities to ensure compliance with data protection requirements including overseeing and regulating the implementation of the law.

Q: Does the law:

- require the designation of a data protection officer? ☐
- require for the DPO to have the power, autonomy and the resources to undertake their mandate? ☐

Notification of breach

Data controllers and data processors have an obligation to notify the supervisory authority and the data subject in case of a data breach within a reasonable time period to be defined by the law.

Q: Does the law:

- require data controllers and data processors to notify:
  - the supervisory authority? ☐
  - the data subject ? ☐
- outline in detail the information which should accompany the breach notification? ☐

Notification should include at minimum details about:

- the nature of the breach,
- those who are affected,
- the likely consequences,
- the measures taken to address the breach and mitigate adverse effects.

Obligations of Data Controllers and Processors

Accountability and enforcement are key to the success of the protection of personal data. The law should clearly identify the parties responsible for complying with the law, as well as their obligations and duties to ensure compliance and protection of the rights of individuals, and what measures they must take should they fail to do so.

The law should clearly define data controllers and processors, and provide clear responsibilities, obligations, and liability for both. The law should also address the relationship between controllers and processors and specify clear requirements as to what is expected of each of them. Controllers and processors should also be subject to record-keeping obligations, security obligations, and data breach notification requirements.

The principle of accountability represents a major evolution in data protection legislation insofar as it puts the burden on data processors to prove that they fulfil their obligations under data protection, including the requirements to keep a record of all processing undertaken under their authority, and to keep that record up-to-date.

Compliance with the Law

Data controllers and processors are responsible for ensuring that they take all necessary measures to ensure that they comply with the law. It is not enough that they comply with the law, but they must clearly illustrate how they are compliant to demonstrate, that processing is performed in accordance with the law. .

Data controllers and data processors should implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with the law.

This may include:

- having an up-to-date data audit/map
- adopting and implementing comprehensive data protection policies and procedures
- taking a by design and default approach
- the appointment of a data protection officer to oversee this process
- having clear ways in which individuals can exercise their rights
- having contracts with those that process data on your behalf or jointly to make sure the obligations are clear

- carrying out privacy/data protection impact assessments
- keeping records of processing activities
- training staff
- implementing strong security measures
- implementing a procedure for responding to, recording, and reporting data breaches
- implementing assessment and evaluation procedures to review and update these measures

Recording Processing Activities

Data controllers and processors should be obliged to keep records of their processing activities as a means of recording (in writing) information that they should be providing to data subjects.

The information could include:

- the name and contact details of the controller(s) and processor(s)
- the purposes of the processing
- a description of the categories of data subjects and of the categories of personal data
- the categories of third-parties to whom the personal data has been or will be disclosed
- the third-parties to whom the personal data has been or will be transferred, including details of safeguards adopted
- the envisaged time limits for deletion of the different categories of data
- a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data

Integrity and Confidentiality

The data controller and the data processor must have the duty and responsibility to safeguard the security of data and the infrastructure. Furthermore, their obligations should require them to report and investigate breaches, as well as to inform the relevant supervisory authority and affected data subjects.

The law should provide security safeguards not only to protect the data itself, but the obligation of protection should be expanded to include the devices and the infrastructure itself used at every stage of processing including generation, collection, retention and sharing (i.e. data at rest and data in transit).

The law should include specific obligations for controllers and processors in relation to the security of processing, including, but not limited to:

- the pseudonymisation of personal data
- the encryption of personal data
- a guarantee of ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly monitoring and evaluation as well as audit of the effectiveness of technical and organisational measures for ensuring the security of the processing, including privacy by design and effectiveness of Data Protection Impact Assessments (DPIAs).

Organisations processing data may also be subject to other legal frameworks, including relating to cybersecurity, which require them to secure data.

Pseudonymisation: Not a Silver Bullet for Complying with Data Protection

Pseudonymisation has been presented as a privacy-enhancing technique which reduces risk and supports efforts of data controllers to comply with their obligations. It means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified without having access to additional information. The purpose is to reduce the linkability of a dataset with the original identity of an individual.

Examples of provisions on pseudonymisation:

As proposed in the draft text for the amendment of Ley 25.326 which regulates data protection in Argentina:

> **“Any processing of personal data so that any information obtained cannot be associated to an identified or identifiable person.”**

Under the GDPR:

> **The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.**

It is important that pseudonymisation is considered as only one among measures a data controller or processor could take: it may not be sufficient on its own, as the very concept hinges on the ability to re-identify and therefore additional measures may be required to ensure compliance with data protection obligations depending on the circumstances. Pseudonymised data is still personal data, and should not be used as a way of circumventing data subject rights, for example by refusing an individual access to their data because they do not have the identifier. For example, where an organisation has allocated an individual a unique ID of which the individual is not aware and therefore is refused access to data associated with that unique ID.

Furthermore, studies have shown that pseudonymisation and standard de-identification alone are not sufficient to prevent users from being re-identified, and there are still risks of data subjects being re-identified.

As noted by the Data Science Institute at Imperial College, London:

> **This combination of pseudonymisation and de-identification worked quite well for about 15 to 20 years. However, modern dataset and especially the datasets used by AI, are very different from those used in the mid 90s. Today's datasets, coming from phones, browsers, IoT, or smart-cities, are high-dimensional: they contain hundreds or thousands of pieces of information for each individual and the way they behave.**
>
> **This fundamentally changes the ability of anonymisation methods to effectively protect peoples' privacy while allowing the data to be used."[1] A study based on mobile phone metadata, showed just 4 points – approximate times and places – are sufficient to uniquely identify 95% of**

> **people in a dataset of 1.5 million individuals. This means that knowing where and when an individual was a mere 4 times in the span of 15 months is, on average, sufficient to re-identify them in a simply anonymized mobile phone dataset, unravelling their entire location history.**

Privacy by Design and by Default

Apart from enforcement through regulation and the courts, technical decisions made in the design stage of systems can play a strong role in putting data protection rules into practice. Through technological means and by considering privacy in the design of systems, it is possible to limit data collection, to restrict further data processing, to prevent unnecessary access, amongst other privacy measures. Laws can influence, and when necessary compel, such developments through a privacy/data protection by design and by default requirement.

Privacy by design

Privacy by design means that data protection must be integrated from the outset when designing a system and so the aforementioned safeguards must be provided from the inception too. The obligation to comply falls on both the data controller and the data processor.

This approach reduces reliance on policy safeguards, but instead regulates processing of personal data through the technology itself. It must be noted that adoption has been slow, as companies and governments are resistant to limit future capabilities or aspirations to mine personal data, even as they are legally supposed to limit 'purpose creep'.

In some jurisdictions, 'privacy by design' has now become a part of a legal requirement. At the 32nd International Conference of Data Protection and Privacy Commissioners in 2010, a resolution was passed which unanimously recognised Privacy by Design as an essential component of fundamental privacy protection.

Privacy by default

A second component is 'privacy by default' which requires that a product, service, or system applies robust privacy and data protection by default. This includes settings that protect privacy by default, i.e. without any manual input from the end user. Such a measure is essential given the cumbersome, complex and highly technical nature of many privacy and data protection policies. The burden should not be on the individual: an individual should not be expected to have the knowledge and expertise to understand the complexity of the services and devices they use. Where possible, they should enjoy the highest level of protection by default.

Impact Assessments

Another requirement that has been integrated into national data protection frameworks is that impact assessments are undertaken prior to processing personal data. This is particularly important where there is a risk to the rights and freedoms of individuals, including where the processing involves sensitive personal data, automated decision-making, profiling, or monitoring of public spaces.

An impact assessment requires, as a minimum:

- an assessment of the necessity and proportionality of the processing
- the risks to individuals
- how these risks are to be addressed.

Data Protection Officers

A key element of any accountability mechanism is oversight. It is important that data controllers and processors clearly designate responsibilities to ensure compliance with data protection requirements. This can include the appointment of data protection officer(s) (DPO), responsible for overseeing and regulating the implementation of the law.

The data controller and processors must ensure that the DPO is provided with adequate power, autonomy and resources to undertake their mandate.

Notification of Breach

Data controllers should have an obligation to notify the supervisory authority and the data subject in the case of a data breach.

This obligation should be clearly stipulated in law and provide:

- Clarity on the time period, which must require notification to occur as soon as possible after the controller/processor is made aware of the breach
- A requirement to notify whenever there is a risk to the rights of the individuals concerned
- What information should accompany the breach notification, such as the nature of the breach, those who are affected, the likely consequences, and the measures taken to address the breach and mitigate adverse effects.

Definitions of 'data breach':

GDPR: "'personal data breach' means 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 [Article 4 (12)]."

Convention 108: "Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects."

The GDPR has made breach notification to a supervisory authority mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals" (Article 33), and to the data subject where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (Article 34). The notification to the supervisory authority must be made within 72 hours of first having become aware of the breach, and to the data subject without undue delay. Data processors will also be required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach. (Article 33, Section 2).

Example of Guidance for Responding to Breaches

In Colombia, when there are security breaches and there are risks to the management of personal data, these must be reported (by both processors and controllers) to the Data Protection Authority.[4] There is an Accountability Guide,[5] which provides that the notification must include the type of incident; the date of the incident; the cause; the type of personal data compromised; and the number of people's whose data was compromised. The guide also provides that those affected should be notified and given the necessary tools to minimise the harm caused by the breach.

International Data Transfers

The overarching approach is that any transfer of personal data to a third country (and any subsequent onward transfer) does not lower the level of protection of individuals' rights to their personal data.

There are various models adopted to regulate and manage the transfer of data across borders. Some jurisdictions, such as Mexico, resort to a privacy notice to be agreed between the data controller and the data subject, which will provide for whether or not the individual agrees for their data to be transferred. The recipient of the data will, in this case, have to comply with the same obligations as the original data controllers. In our opinion, this model is not satisfactory.

A common mechanism for regulating and overseeing international data transfers is an assessment of the adequacy of the expected recipient of the data. This is the model taken in Europe and Argentina, for example.

Under this model, any sharing or transfer of personal data to entities in other countries is allowed, if the recipient of the data provides a level of protection of personal data that is, at a minimum, equivalent to the level established in the national law of the sender. The assessment can be conducted by an independent supervisory authority/Data Protection Authority, following open consultation and thorough investigation.

The assessment of the level of protection of personal data afforded in the third country should include explicitly:

- Respect for human rights and fundamental freedoms, relevant legislation, including concerning public security, defence, national security and criminal law, and the access of public authorities to personal data
- Recognition of the rights of citizens and foreigners within the territory, without discrimination on the basis of immigration status
- Rule of law, including national legislation in force and regulatory/ professional rules;
- Existence and effective functioning of independent supervisory authorities to ensure compliance with the law
- The international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Decision-making mechanisms should be open, clear, prescriptive, and involve consultation with relevant actors including civil society. Furthermore, this assessment should be reviewed regularly, to provide a periodic review mechanism of the decision-making process.

If an adequacy assessment cannot be undertaken, the controller or processor should take measures to compensate for the lack of data protection, ensuring that the appropriate safeguards exist and are enforceable in order to protect the data subject. Appropriate safeguards may take various forms: examples from the EU have included developing binding corporate rules for intercompany transfers, and standard data protection clauses within contractual clauses, as authorised by a supervisory authority.

Examples of Adequacy Mechanisms

Under Article 45 of Regulation (EU) 2016/679 (GDPR), the European Commission provides for a mechanism by which to determine whether a country outside of the EU offers an adequate level of data protection and, if accepted, whether to allow data to flow from the EU to that third party without any further safeguards.

The adoption of an adequacy decision involves 1) a proposal from the European Commission, 2) an opinion of the of the European Data Protection Board, 3) an approval from representatives of EU countries, and lastly 4) the adoption of the decision by the European Commissioners.[6]

While Section 12 of Argentina's Data Protection Law 2000 No. 25.326 ('the Law'), prohibits transfers to countries that do not provide adequate levels of protection, the adoption of a Regulation in 2016 introduces two model contracts for international data transfers to countries that do not provide adequate levels of protection with one applying for transfers by data controllers to data controllers, while the other must be used for transfers to data processors rendering services.[7]

In South Africa, the law provides for a set of conditions which must be complied with by the 'responsible party' (the sending party) to transfer personal data about a data subject to a third party in a foreign country. These include that (i) the data subject must consent to such a transfer; (ii) the transfer is necessary for the performance of a contract; and (iii) the transfer is for the benefit of the data subject and it is not practical for the responsible party to obtain the consent of the data subject for that transfer.

Exceptions

There are various reasons for data transfers to occur, which may be seen as being exempt from compliance with data protection:

- When the transfer is necessary for international legal cooperation between public intelligence and investigation bodies, in accordance with instruments of international law and with the respect to principles of legality, necessity, and proportionality;
- When the transfer is necessary for the protection of the data subject's or a third party's life or physical safety;
- When the competent body authorises the transfer under the terms of the regulations;
- When the transfer is the result of a commitment assumed in an international cooperation agreement; and
- When the transfer is necessary for the execution of public policy, or falls within a public authority's legal mandate.

Irrespective of the exceptions deployed, these need to be highly regulated and will require further guidance to ensure that they are not broadly interpreted or open to abuse, and are compliant with human rights standards. These exceptions must be narrowly-framed and interpreted to ensure that such agreements do not result in the weakening of the data protection offered in the law.

References

1 de Montjoye et al, 'Solving Artificial Intelligence's Privacy Problem', Imperial College London Data Science Institute, February 2018, available (PDF) at: https://www.imperial.ac.uk/media/imperial-college/data-science-institute/WhitePaper_SolvingALPrivacyIssues.pdf

2 d de Montjoye et al, 'Unique in the crowd: The privacy bounds of human mobility' 3, 1376., Scientific Reports Volume 3, Article number: 1376 (2013), available at https://rdcu.be/WBtA

3 Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010, available at: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

4 Articles 17(n) and 18 (k) of Law 1581/2012 available at: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

5 Industria y Comercio, Guia para la implementacion del principio de responsabilidad demonstrada (Accountability), p20, available (PDF in Spanish): https://iapp.org/media/pdf/resource_center/Colombian_Accountability_Guidelines.pdf

6 European Commission, 'Adequacy of the protection of personal data in non-EU countries', available at:https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

7 8 November 2016, Regulation 60 – E/2016 on international transfers of personal data

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 7:

Independent Supervisory Authority

Independent Supervisory Authority

While international data protection agreements remain largely non-prescriptive on enforcement, in order to give effect to the fundamental right of data protection and its principles, legislation must provide for the establishment of an independent supervisory authority. A supervisory authority requires this statutory footing in order to establish clearly its mandate, powers and independence.

Models and Structures

Two models of enforcement have been considered: the creation of an independent supervisory authority, and a ministry-based model.

Of the seven international agreements and standards relevant to data privacy, five require the establishment of an independent supervisory authority. While the OCED Principles did not call for an independent supervisory authority, the EU model, both the GDPR (previously Directive 1995) and the Convention 108 of the Council of Europe, did - 90% of countries with data protection laws have opted for this model. Having an independent supervisory authority is also directly relevant to an assessment of adequacy as it is essential for oversight and enforcement.

However, it is important to note that in many jurisdictions, such as Mexico and the UK, a single institution has been set up to serve both as a regulator and enforcer of laws pertaining to access to information and data protection. This combination of functions should not contradict the mandate, functions and powers of the enforcement authority, or independence from the Executive.

Furthermore, some countries have opted to have multiple independent supervisory authorities. In Germany the regulation of data protection in relation to public and private bodies happens at the state level, and then there is a Federal Data Protection Commissioner which monitors federal authorities and other public bodies under federal government control.

Structure, Mandate and Powers

The mere establishment of this independent authority is not sufficient. The law must ensure the following:

Structure

- Process for establishment and appointment: The law should provide for a process and timeframe for the establishment of the authority and appointment of its head/ members.
- Composition and structure: The law should lay out the composition of this authority, including the skills and expertise required.
- Resources: The law must stipulate that the authority will be given sufficient resources, both financial, technical and human.
- Independent status: The law must stipulate that the independent data protection authority remains independent, in order to effectively and adequately fulfil its mission of enforcing the data protection framework.
  The authority should be free from external influence, and refrain from actions incompatible with the duties of the authority.
- Monitor and enforce: The authority must be given the task to monitor and enforce the application of the law. This would also require periodic review of activities of those who are subject to the law.

Mandate

- Mandate to investigate: The authority must be given the mandate to conduct investigations and act on complaints, by issuing binding orders and imposing penalties when it discovers that an institution or other body has broken the law. This includes being able to: demand information from the controller or processor, conduct audits, obtain access to all the information they may need for the purpose of the investigation, including physical access to premises or equipment used for processing, if necessary.
- Mandate to receive and respond to complaints: Both individuals and public interest/privacy associations should be given the right to lodge complaints with this independent authority. The independent authority should also be able to receive complaints of competent organisations based on evidence revealing bad practice before a breach has occurred.

- Mandate to provide advice: The authority should advise the relevant government bodies (depending on political system), as well as other public bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regards to the processing of their personal data.
- Provider of information: The work of the authority should include the provision of information to data subjects with regards to the exercise of their rights under the law in their country or elsewhere; the latter may require liaising with foreign supervisory authorities.
- Mandate to promote public awareness: Part of the role of the authority is to promote public awareness and understanding of data subjects' rights, risks, rules, and safeguards. This includes awareness of the recourses available to them for demanding and enjoying those rights, and the risks to be conscious of when it comes to the protection of personal data.

Power

- Power to impose sanctions: The independent authority must have the power to impose appropriate penalties, including fines, enforcement notices, undertakings, and prosecution. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.
- Issuing recommendations and guidelines: Derived from its power to investigate and impose sanctions, the independent data authority should also be capable of issuing recommendations and guidelines, outlining its interpretation of some provisions or aspects of a data protection law, either in general or directed to a specific sector. Given the fast pace of technological development, this is also a way to avoid data protection laws becoming outdated and obsolete.
- Special regulatory powers: Additionally, in some cases a data protection law can give the data authority powers to regulate certain aspects of the law, for example to update definitions, security requirements, and approve trans-border data flows.

Taking action when the law is broken

The types of sanctions/ penalties which could be imposed vary, but may include:

- Administrative Fines, For example, under the GDPR, fines are set at €20, million or 4% of annual turnover; in South Korea, it is 3% of annual turnover.[1]
- Criminal offences (individual responsibility) for certain actions, for example knowingly or recklessly, without the consent of the data controller, obtaining or disclosing personal data.
- Direct liability for directors of companies

References

1 2014-2017 Update to Graham Greenleaf's Asia Data Privacy Laws: Trade and Human Rights Perspectives, University of New South Wales Law Research Series, 2017

PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 8:

Annex: Resources

Reference Documents

Privacy International

Explainers

Video: What is data protection? Video https://www.privacyinternational.org/video/1623/video-what-data-protection

Explainer: What is data protection? https://www.privacyinternational.org/explainer/41/101-data-protection

What is GDPR?: https://privacyinternational.org/topics/general-data-protection-regulation-gdpr

Educational resources

Online course: Right to Privacy: Introduction and Principles https://advocacyassembly.org/en/courses/28/#/chapter/1/lesson/1

Online course: Right to Privacy: Data and Surveillance https://advocacyassembly.org/en/courses/22/#/chapter/1/lesson/1

Online course: The Risks of Data-Intensive Systems https://advocacyassembly.org/en/courses/41/#/chapter/1/lesson/1

Advocacy and policy analysis

What we do: Modernise Data Protection Law https://privacyinternational.org/what-we-do/modernise-data-protection-law

Topics: Data Protection https://privacyinternational.org/topics/data-protection
National and international legal and policy analysis https://privacyinternational.org/how-we-fight/advocacy-and-policy

Research and investigations

State of Privacy: https://privacyinternational.org/type-resource/state-privacy

Invisible Manipulation - 10 ways our data is being used against us: https://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-being-used-against-us

Other Organisations/Bodies

Specialised organisations and networks

European Digital Rights (EDRi): https://edri.org

Trans Atlantic Consumer Dialogue: https://tacd.org

Consumer International: https://www.consumersinternational.org

International Association of Privacy Professionals (IAPP): https://iapp.org/resources/ IEEE https://www.ieee.org/publications/index.html

European Union Fundamental Rights Agency

Theme - Information society, privacy and data protection: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Handbook on European data protection law, June 2018: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

United Nations

Economic and Social Council, Human Rights and Scientific and Technological Developments, Note by the Secretary-General, E/CN.4/1233, 16 December 1976: https://digitallibrary.un.org/record/559884/files/E_CN.4_1233-EN.pdf

General Assembly UN Guidelines on the regulation of computerized personal data files: http://www.un.org/documents/ga/res/45/a45r095.htm

The Right to Privacy in the Digital Age: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Legal analysis

DLA Piper, Compare data protection laws around the world and Handbook: https://www.dlapiperdataprotection.com

National, regional and international regulatory bodies

Council of Europe: http://www.coe.int/en/web/data-protection/home

Data protection in the European Union: http://ec.europa.eu/justice/data-protection/

Article 29 Working Party (now dissolved and replaced by the European Data Protection Board): http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Organisations of American States: http://www.oas.org/dil/data_protection.htm

Association francophone des autorités de protection des données personnelles (AFAPDP): https://www.afapdp.org/documents

International Conference of Data Protection and Privacy Commissioners: https://icdppc.org/document-archive/

Red Iberoamericana de Protección de Datos (RIPD): http://www.redipd.es/documentacion/index-ides-idphp.php

Asia Pacific Privacy Authorities (APPA): http://www.appaforum.org/resources/

Academia

Brussels Privacy Hub, Vrije Universiteit Brussels: https://www.brusselsprivacyhub.eu/index.html

International Data Privacy Law (DIPL), Oxford University Press: https://academic.oup.com/idpl

Graham Greenleaf, University of New South Wales, Faculty of Law, Australia: https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=57970

Avenues for Engagement

There are a variety of opportunities for civil society organisations interested in engaging in promotion and protection of the right to privacy of individuals and the protection of their data. This is not an exhaustive list, but below are various avenues for engagement at the national and international level which we hope will encourage more civil society organisations from across disciplines to engage in policy developments and legal processes on data protection.

National

Civil society organisations

Civil society organisations must have a seat at the table to ensure that policy-making processes are open, inclusive and transparent. It is important that more diverse organisations can join the campaign for privacy and data protection. Civil society organisations whose mandate is to promote and advocate for the protection of fundamental rights play a crucial role in undertaking independent research, investigation as well as policy and legal analysis of current and proposed practices and policies on data protection. These collaborative efforts play a crucial role in informing and educating relevant actors to ensure the highest privacy and security standards and measures are adopted and enforced, and public and private institutions comply with their national and human right obligations.

Through our work with the Privacy International Network we have engaged for over a decade to advocate for the adoption of data protection laws across the world. Find out more about the Privacy International Network: https://privacyinternational.org/partners.

Independent supervisory authorities

Where they are in place, independent supervisory authorities, often known as national data protection and/or privacy authorities, have the mandate and responsibility of giving effect to and ensure compliance with the data protection legislation. As the debate evolves on data protection engagement with these authorities is essential to ensure their understanding of the new challenges posed by new technologies and systems as well as the implications for the protection and promotion of fundamental rights. Through public consultations organised by the authority as it develops new policies, guidelines and standards, there are opportunities for CSOs to share their concerns and recommendations.

Legal community, judiciary and legal institutions

One avenue for engagement is awareness-raising and training amongst the legal community, both with lawyers and judges, which is essential to ensure a well-informed and well-equipped judiciary that is increasingly required to consider cases of privacy violations and situations involving more advanced technologies

and innovations. Secondly, strategic litigation provides a unique opportunity to challenge existing laws and practices, and to call for reform to ensure that laws are in line and interpreted with respect to national, regional and international human rights standards. The norms set and strengthened by courts provide strong advocacy opportunities in ensuring they are implemented in accordance with the law but also as means of raising-awareness amongst society as to their rights.

National human right institutions

In countries where governments and courts are failing to uphold the rule of law, national human right institutions (NHRIs) play an important role as guardians and watchdogs of human rights. As we highlighted in our guide, data protection is tightly linked to the promotion and protection of the right to privacy. The right to privacy is multi-faceted, but a fundamental aspect of it, increasingly relevant to people's lives, is the protection of individuals' data. Therefore, engagement with NHRIs is essential to ensure that interferences with and violations of data protection and the right to privacy are researched, documented and acted upon. This requires raising awareness on the challenges faced by the development and use of new technologies if they are deployed in a legal void with poor or no regulatory mechanisms and/or human rights considerations. CSOs provide an important source of information to these institutions in order to guide investigations and monitoring strategies, and to set their priorities.

Sectorial regulatory bodies

Many countries have a variety of regulatory bodies which oversee the effect implementation of sectorial laws and/or policies which may include (or lack) privacy and data protection provisions. For example, telecommunications regulators, who are playing increasingly important roles in areas around communications surveillance and spectrum management of tactical surveillance techniques. Increasingly electoral commissions as well as welfare and social affairs agencies are becoming proponents of the deepening of databases and invasiveness of identity systems. CSOs can play helpful roles in increasing their understanding of the new challenges posed by new technologies and systems.

Ministries and legislative bodies

A variety of Ministries and legislative bodies are developing laws and policies around technology policy every day that have significant implications for the governance of personal data and the protection of fundamental rights. However, often a lack of appropriate laws to protect privacy and therefore no governance framework for them to consider. In many countries, this legal void means there are no, or few guarantees for protection, and avenues for redress are non-existent or inefficient. Through providing expertise informed by capacitation and having conducted their own research, civil society plays an important role in presenting and consolidating information on the practical human rights implications of current policies to government ministries, agencies, and Parliamentary committees and bodies responsible for drafting and reforming laws.

Regional and international

United Nations bodies

Some human right bodies have the mandate capacity to monitor and provide recommendations and redress. Particularly giving their open and consultative approaches, they provide an important space for civil society to engage and convey their concerns, and challenges they face at the national level as result of national but also regional and international policies and practices, and advocate for change in their respective countries. They are various opportunities to raise issues related data protection and privacy in some of UN treaty bodies as well as human right monitoring and reporting mechanisms as outlined in Privacy International's Guide "How To Talk About Privacy at the UN? https://privacyinternational.org/feature/1030/brief-guide-how-talk-about-privacy-un.

Consultative Committee (T-PD) of the Convention 108 Of the Council of Europe

Established by Convention 108, the Consultative Committee (T-PD) consists of representatives of Parties to the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data complemented by observers from other States (members or non-members) and international organisations, and is responsible for interpreting the provisions and for improving the implementation of the Convention. The Consultative Committee of Convention 108 is also responsible for drafting reports, guide lines and guiding principles on such topics as, the contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection or data protection with regard to biometrics. To find out more visit: https://www.coe.int/en/web/data-protection/consultative-committee-tpd.

International Conference of Data Protection Commissioners (ICDPPC)

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) was established in 1979 with the vision of an environment in which privacy and data protection authorities around the world are able effectively to fulfil their mandates, both individually and in concert, through diffusion of knowledge and supportive connections. Organised annually, the Conference has The Conference has set itself four high level priorities to allow actions to be focused and more effective: 1) strengthening our connections, 2) working with partners; 3) advancing global privacy in a digital age; and 4) completing conference capacity building and assessing our effectiveness. As the second strategic plan these priorities are aimed at enhancing the Conference's capacity for action. The Conference adopts various resolutions and issues declarations which present the key outcomes of the conference and outline upcoming project to be undertaken by the Secretariat as well as national data protection authorities. To find out more visit: https://icdppc.org.

Association francophone des autorités de protection des données personnelles (AFAPDP)

The AFAPDP was set-up on 2007. It brings together independent data protection authorities from 19 States which share a language, a legal legacy and shared values. The vision of the ADAPDP is to promote the adoption of measure to effectively and efficiently safeguard the right of persons to data protection. It aims to contribute to guarantee the fundamental rights of individuals which promotes a Francophone digital space based on trust suitable for economic development. It works to reinforce the capacity of members of the AFAPDP, to encourage researching and sharing best practices, to act as a hub of expertise, to collect and disseminate information about its members, and to cooperate with other organanisaitons to promote data protection and democracy. The AFAPDP meets annually for its general assembly and it also organises an annual conference, and field visits are conducted in member countries to explore a specific country and/or issues. To find out more visit: https://www.afapdp.org.

Red Iberoamericana de Protección de Datos (RIPD)

The Red Iberoamericana de Protección de Datos (RIPD, Ibero-American Data Protection Network) was established in 2003. The aim of the RIPD is to promote collaboration, dialogue and share information, promote policies, methodologies to ensure It currently consists of 22 Data Protection Authorities (DPAs) from Spain, Portugal, Mexico, and other countries in Central and South America and the Caribbean. Over the last decade, the organization has promoted the development of comprehensive data protection legislation and the introduction of data protection authorities throughout Latin America. The RIPD promotes dialogue and drives agenda-setting initiatives through the organisation of annual meetings, seminars, and workshops, as well as the production of standards and principles to support DPAs and other stakeholders engaging on data protection. To find out more visit: http://www.redipd.es/index-ides-idphp.php.

Asia Pacific Privacy Authorities (APPA)

APPA is a forum for data protection and privacy authorities in the Asia Pacific region. It gives the authorities in the region an opportunity to form partnerships, discuss best practices and to share information on emerging technology, trends and changes to privacy regulation. APPA members convene twice a year, discussing permanent agenda items like jurisdictional reports from each delegation and an initiative-sharing roundtable. At each forum, members discuss and focus on different topical issues. To find out more visit: http://www.appaforum.org.

The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is established by the General Data Protection Regulation (GDPR), and is based in Brussels. It is composed of representatives of the national data protection authorities and the European Data Protection Supervisor. The EDPB

aims to ensure the consistent application in the European Union of the GDPR and of the European Law Enforcement Directive. The EDPB can adopt general guidance to clarify the terms of European data protection laws, giving stakeholders a consistent interpretation of their rights and obligations. They are also empowered by the GDPR to make binding decisions towards national supervisory authorities to ensure a consistent application. To find out more visit: https://edpb.europa.eu/edpb_en.

Central and Eastern Europe Data Protection Authorities

Founded in 2001, the Central and Eastern Europe Data Protection Authority links the national institutions responsible for personal data protection policy in 17 states in Central and Eastern Europe. It hosts an annual meeting and publishes recommendations and positions on the implementation of data protection laws. Its online platform is designed to support the activities for close co-operation and mutual help between these data protection authorities. To find out more visit: http://www.ceecprivacy.org/main.php.

Other Relevant Stakeholders

Industry

Economic actors have emerged as influential, powerful actors in the global economy. In many commercial sectors, including the mining and extractive industry, such actors have come under increased scrutiny, being imposed to conduct and implement human rights assessments, but this is yet to be mainstreamed across the industrial sector. Whilst ultimate responsibility does fall upon governments to guarantee citizens enjoy their fundamental human rights, which includes protecting them from the action of third parties, some of the responsibility does fall onto industry. Civil society can play a role in raising awareness about the right to privacy and the risks that emerge from commercial activities of industry. If reached out to effectively, industry could become an ally to ensure the protection of rights by ensuring they do not collude with and are not pressured into unlawful practices.

Technology community

This community includes individuals and groups that design new technologies but also security researchers and hackers. Whilst much of the debate lies with the poor governance and regulation of these technologies rather than the tech itself, this is a potential ally community which must be further engaged with. By working with the tech community, CSOs can identify and prescribe standards for promoting privacy by design approaches to innovation particularly to enable information governance.

Media

The media plays a crucial role in monitoring, investigating and information sharing. They are also often a great force as the watchdogs of democracy and good governance. Traditional forms of media remain a very strong source of information for the public particularly in countries where access to the internet is not as easily accessible and reliable.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471