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.

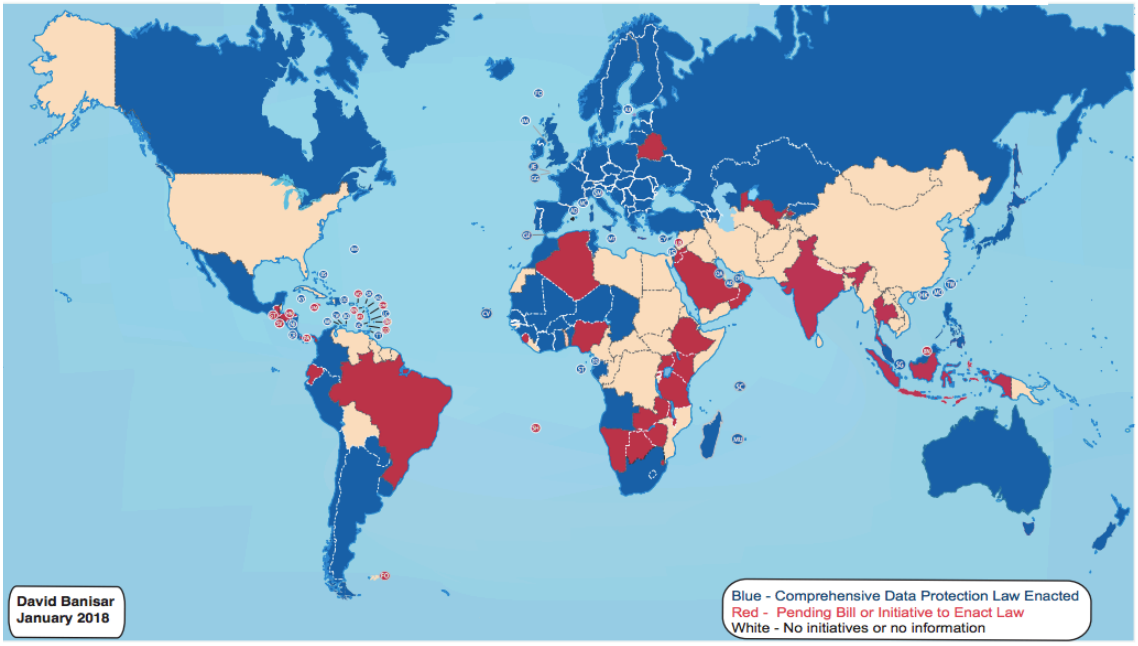
Redress for breaches of data protection law should also be available through the courts, both through individual actions and collective redress (brought by NGOs and consumer groups).

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