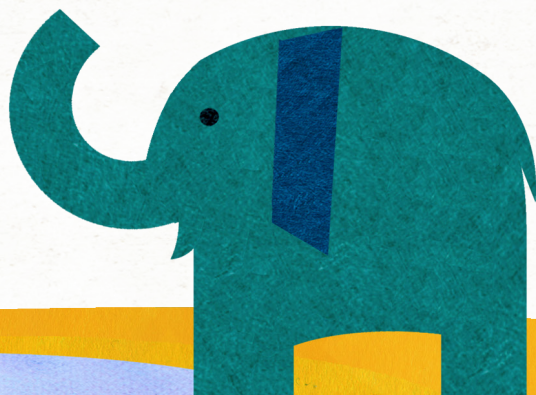


TRAVEL GUIDE TO THE DIGITAL WORLD:  
**DATA PROTECTION  
FOR HUMAN RIGHTS  
DEFENDERS**







Published in London 2018  
by Global Partners Digital



This work is licensed under Creative Commons,  
Attribution-NonCommercial-ShareAlike



“Data is the pollution  
problem of the information  
age, and protecting privacy  
is the environmental  
challenge”

Bruce Schneier







The phrase “data is the new oil” has become a cliché.

But it points to something real. In the digital age, the processing of personal data has become a hugely valuable and lucrative activity. It offers undeniable opportunities for economic growth, social advancement and research. It can also, without adequate safeguards, pose risks to the rights of individuals – particularly their right to privacy.

Since the 1980s the processing of personal data has been regulated by a set of frameworks known as data protection. Over 100 countries around the world now have data protection legislation, but the extent of coverage varies widely. At the same time, the fragile balance which the original data protection principles sought to preserve – allowing free flow of data while also preserving user rights – is being tested by technological developments which have radically increased the scale and depth of personal data processing.

Maintaining this balance in the age of technologies like the internet of things and artificial intelligence is going to be a crucial focus for policymakers in the coming years, both at the national level and in international forums. To ensure that the policies and laws which emerge are rights-respecting, it's crucial civil society are able to engage in an informed and effective way.







## OVERVIEW

The aim of this guide is to equip human rights defenders with the information they need to be able to engage with, advocate to, and inform policymakers on data protection.

**CHAPTER 1** covers what data is, setting out a brief history of personal data, its uses in the digital age, why it's vulnerable, and why it needs to be protected.

**CHAPTER 2** turns to the debate surrounding data protection, looking at the relevant stakeholders and their interests, and examining the proposed approaches to regulating personal data in the digital age.

**CHAPTER 3** looks at the links between data protection and human rights, particularly the right to privacy.

**CHAPTER 4** sets out the components of human rights-respecting regimes on data protection.

**CHAPTER 5** introduces and examines the various forums – at the international, regional, and national levels – where data protection standards are set.

**CHAPTER 6** sets out some of the messages and strategies human rights defenders can use to advocate for data protection in different contexts and within different data protection regimes.



# CONTENTS

## CHAPTER 1

### WHAT IS DATA PROTECTION?

II

What is personal data?	12
What is data processing?	14
Why personal data needs protection	16
A short history of data protection	17
Types of data protection regimes	20
Data protection and the internet	22

## CHAPTER 2

### THE DEBATE

25

Different approaches to solving the problem	26
The debate in the real world	30
The stakeholders	32

## CHAPTER 3

### WHY IS DATA PROTECTION A HUMAN RIGHTS ISSUE?

37

The right to privacy	38
Data protection and privacy	42
Data protection and other human rights	46
Human rights in conflict?	48



CHAPTER 4

**WHAT WOULD A HUMAN RIGHTS-RESPECTING  
DATA PROTECTION REGIME LOOK LIKE?** 51

CHAPTER 5:

**WHERE ARE DATA PROTECTION STANDARDS SET?** 61

Binding data protection standards 63

Non-binding data protection standards 69

CHAPTER 6:

**HOW CAN HUMAN RIGHTS DEFENDERS AND  
CIVIL SOCIETY ORGANISATIONS ENGAGE?** 81

Countries with weak or sectoral data protection regimes 82

Countries with a comprehensive data protection regime 84

**GLOSSARY** 87

**APPENDIX** 89

Annex 1 89

Annex 2 92







# CHAPTER I

# WHAT IS DATA PROTECTION?





## What is data protection?

Almost every aspect of daily human life – from business, to leisure, to the usage of public services – now relies at least to some extent on the processing of data: its collection, storage, use, and dissemination.

Data protection, the subject of this guide, refers to the regulation of the processing of one type of data in particular – **personal data**.

The processing of personal data has the potential to make our lives better and easier. At the same time, it can also pose risks, including to human rights.

In this chapter, we set out what we mean by personal data and **data processing** and why processing of personal data in particular needs to be regulated. Then we examine the origins and history of data protection and consider how the advent of the internet has created new challenges for its implementation.

## WHAT IS PERSONAL DATA?

Data is any kind of information which is recorded in some way. It can exist online or offline, in forms which are intelligible to humans or only readable by computers.

Not all data is personal data. A sensor in a factory measuring the number of cans of beans being produced per hour is not processing personal data. Even though this data may have great economic or social value (and its loss or damage could cause significant harm), it is not until that data relates to an identified or identifiable person – the **data subject** – that it qualifies as personal data. The person or entity which collects and processes personal data is known as a **data controller**.



## A word on terminology

When it comes to data protection, the existence of different legal systems and cultures means that there are different terms used to mean or refer to the same or related things. Take data protection itself, for example. In some places, it is referred to as “data privacy.” We use the term data protection here but it should be seen as interchangeable with data privacy.

The same goes for the term data controller. In some parts of the world, the term “data steward” or even “responsible party” is used. We use the term data controller. The term “data processor” is also used in some data protection regimes, such as the EU’s, but is different. A data processor is anyone who processes personal data on behalf of a data controller. In this guide we don’t refer to data processors because the distinction between data controller and data processor doesn’t exist worldwide. We use the term data controller to refer to any person or entity which collects and processes personal data, as this term has an equivalent term in all data protection regimes.

While information about people, or information that can lead to a person’s identification, has existed throughout human history, the concept of personal data was only formally defined in the 1970s with the advent of the first digital technologies. And the basic elements of this definition have remained more or less consistent up to the present day: personal data is simply any data which relates to an identified or identifiable individual.

There are broadly four categories of data which fall under this definition.

- Information which explicitly identifies an individual. This might mean, for example, a full name, an email address which contains the user’s full name, or records of a person’s face.



- Information which does not explicitly identify an individual by itself, but is unique to an individual and enables them to be identified, if further information is considered alongside it. This might be a telephone number, a national identification or passport number, or a set of fingerprints.
- Information which may not be unique to an individual, but is possessed only by a small number of people, such as dates of birth and IP addresses, which could identify individuals if combined with other data.
- Information which does not identify a person as such, but provides information about a person or their activities. This could include information relating to a person's health or their employment records. Or it could be geolocational data, their search history, social media activity, or their online purchases.

## WHAT IS DATA PROCESSING?

Broadly speaking, data processing refers to the collection, storage, use, or dissemination of data. While definitions vary, below is an explanation of what each of these types of data processing refers to.

- **Collection:** Or, in other words, getting the data. Data collection can be relatively manual and simple – for example, having a person fill out a form or a survey. But data can also be collected completely automatically by machines, without the data subject or a specific human **data controller** being aware of it – for example, through a web browser or a surveillance camera.
- **Storage:** Once collected, personal data has to be kept somewhere. This might be in a filing cabinet, on a database, or in a **cloud**-based application.
- **Use:** This covers the various operations which might be performed on data. For example, comparing it to other databases, making data anonymous, converting it into a different file format, or ordering it in a different way.



- **Dissemination:** This refers to the ways in which data is shared with others. For someone working in a business, disseminating data might mean exporting a database of customer information into a spreadsheet, or presenting it in a PowerPoint. Or it might mean a social media company sharing information collected about user behaviour with advertisers.

The processing of data – both personal and non-personal – has the potential to improve people's lives. It can make services better, foster breakthroughs in medicine and public health, and create better products and services. The qualities that make the processing of data useful can, however, also create risks. If the data is lost or exposed, this can risk harm to individuals, systems, companies, and even states.

Data protection is specifically concerned with the processing of personal data, which carries particular and specific risks. Personal data can reveal who a person is, their relationships, health status, and history, financial details, sexual preferences, and beliefs. Its processing can therefore pose serious risks to a person's **right to privacy**.

The right to privacy, as we'll see in chapter 3, is protected in various legal instruments at the national and international levels. The processing of non-personal data, because it cannot impinge on the right to privacy, is not covered by data protection frameworks although it may be governed through various other regulatory and non-regulatory frameworks, like laws that protect trade secrets, or cybersecurity policies or laws, for example.





## WHY PERSONAL DATA NEEDS PROTECTION

Data has been collected, stored, used, and disseminated throughout history. The ancient Roman census, for example, saw administrators going door to door to gather information on citizens, ranging from the size of their household to the amount of land owned. However, the development of the computer in the 1950s, and the increasing use of them in the 1960s, changed the nature of the processing of personal data, and the extent of the need to protect it.

Even before the internet, the computer had already revolutionised the ways that records and data were collected, stored, used, and disseminated:

- **Collection:** In the early days of computing, most data was still collected and inputted manually into computers. This was done via keyboards or punch cards (a way of recording data on cards in a radically shortened form). These advances in keyboards and punch cards made the collection of data much faster and easier.
- **Storage:** One of the main attractions of computers was that they could store vast amounts of data. Early computers did this through punch cards or magnetic tapes which were able to store more data than had been traditionally possible through paper. As computers got steadily more advanced, they were able to store larger amounts of data in increasingly smaller spaces, and at lower cost.
- **Use:** Computers – initially used mainly for military applications – were, by the 1960s, increasingly being used to automatically process and store data by certain large companies and governments. This trend was to continue throughout the 1970s and 1980s, which saw radical advances in data storage and processing, and the gradual incorporation of digital technologies into a range of day-to-day activities – including communications, shopping, finance, and healthcare.



**Dissemination:** Computers made it much easier to share data, including across borders. Even before they were networked, the use of floppy and hard disks allowed the compression of large amounts of data into small objects, which could be easily shared.

These developments – and the risks associated with them – led to public concerns in the 1960s, in particular in the United States and in Europe, where computers were beginning to be widely used at that time. Books and pamphlets regularly prophesied “the end of privacy”. While privacy laws already existed, they were broad and undefined, and did not offer much guidance on what to do about protecting the right to privacy when so much personal information was being processed.

## A SHORT HISTORY OF DATA PROTECTION

In response, governments in both the United States and Europe agreed that there was a need to regulate the processing of personal data. They set up “expert committees” to investigate the question, which ended up enumerating a set of guiding principles that came to underpin all future data protection frameworks, and have since been codified in two international level texts: the Organisation for Economic Co-operation and Development (OECD) guidelines on the protection of privacy and transborder data flows, and the Council of Europe's Convention 108 (see chapter 3).

These guiding principles are best understood as seeking a balance between two distinct priorities: respecting the rights of citizens, while also retaining the ability to process personal data for economic and social purposes.



# Key dates in the evolution of data protection in the U.S. and Europe (1970-2018)

## 1970

- The German federal state of Hesse passes the world's first data protection law

## 1973

- Sweden passes a data protection law
- The Council of Europe passes a Resolution on the Protection of the Privacy of Individuals in relation to Electronic Data banks in the Private Sector
- The US Department of Health committee issues a Code of Fair Information Practice

## 1980

- The OECD publishes Guidelines on the Protection of Privacy and Transborder Flows

## 1981

- The Council of Europe adopts the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)
- The Netherlands passes the Act on Personal Data Registrations

## 1990

- The UN General Assembly adopts Guidelines for the Regulation of Computerised Personal Data Files

## 1995

- The EU passes the Directive on Data Protection





1974

- The Council of Europe passes Resolution on the Protection of the Privacy of Individuals in relation to Electronic Data Banks in the Public Sector
- The United States passes the Privacy Act


1977

- Germany passes the Federal Data Protection Act

1978

- Norway passes the Data Registers Act
- Denmark passes the Private Registers and Public Registers Act

1984

- The United Kingdom passes the Data Protection Act
- 

2013

- The OECD updates the 1980 set of Guidelines on the Protection of Privacy and Transborder flows

2016

- The EU passes the General Data Protection Regulation (GDPR)

2018

- The GDPR comes into force across all EU member states
- 



In particular, two elements were identified as key means to achieve this balance:

- **Imposing obligations on data controllers.** An example is the obligation to specify the purposes for which the personal data is being collected at the time it's being collected, to store data securely and to dispose of data once it is no longer relevant for the purposes it was originally collected.
- **Providing data subjects with rights.** This would allow them to control the collection and processing of their personal data.

These two elements came to be incorporated in legislation in countries across the world, setting the foundations of what we now know as data protection: the regulation of the collection, storage, use, and dissemination of personal data once it has been volunteered by a data subject, or obtained by a data controller.

## TYPES OF DATA PROTECTION REGIMES

Despite agreement on the basic principles of data protection and means to implement them, there are significant differences in how these are applied in practice, resulting in a multitude of competing data protection regimes across the world. Regimes can be defined as the set of standards (or principles, norms, and rules) and the decision-making procedures which determine the behaviour of any institution – including a government – on a given issue.

Data protection regimes differ from country to country and can be either comprehensive or sectoral:



- **Comprehensive:** If a country has “comprehensive data protection”, this means that the legislation applies to personal data processed by any entity in that country, whether it is public or private, regardless of sector.
- **Sectoral:** In some countries, regulation only applies to data processed by the public or private sector. In other countries, regulation only applies to particular fields of industries within the public or private sector that process data (e.g. healthcare or education).

There are many reasons why these differences in data protection regimes exist. Some are due to divergent legal and political cultures. In the US, for example, a comprehensive data protection regime has long been resisted because of political resistance to an approach which would impose greater state control on market actors. This is in contrast to European countries where the comprehensive approach can be found and there is, in general, longstanding support for regulatory responses or approaches to policy challenges.

In some cases, resource constraints may be the crucial factor. Data protection frameworks are a relatively recent phenomenon, having only arisen in the last 40 to 50 years, and may not be seen as a top priority for states where policymaking capacity is already overstretched. In some countries, existing legal protections for the right to privacy are seen to be sufficient to cover data protection issues.

Other more specific reasons can explain the uptake of data protection in certain regions. The recent uptake of comprehensive data protection in West and North Africa (from 2013 to 2018, ten countries in these regions adopted data protection frameworks) is partly credited to the existence of a network of data protection authorities supporting cooperation and training initiatives between Francophone countries in the field of data protection.



## DATA PROTECTION AND THE INTERNET

The rapid spread of the internet has created new challenges around the application of data protection. In particular, it has made user rights more difficult to exercise. This is for two reasons:

- **Growing complexity of data flows:** According to the principles of data protection, data controllers should be accountable for, and transparent about, their processing of personal data. For example, users have the right to know what data is held about them and be able to amend or delete that data, subject to certain conditions. The increasing complexity of data flows, however, is making fulfilling that obligation more difficult. Increasingly, personal data moves through multiple jurisdictions, which may have different obligations. For example, someone may be using a taxi service operating via an online platform in Ghana, but the personal data relating to their trips may be processed by a company whose offices are headquartered in the US, who in turn uses a company who provides global data storage services. This could mean their data ends up being stored anywhere from Ireland to Hong Kong to India, all of which have different data protection frameworks.
- **The difficulty of obtaining meaningful consent:** In the digital age, the automatic generation of personal data has greatly increased, and the automated collection and processing of personal data has become much cheaper and routine. This means that making sure that users can exercise their rights over their data is much more challenging. One of the reasons is that the sheer scale of data collection has meant that data controllers have traditionally relied on “tick-box” **terms of service** agreements (TSAs) to get consent for the collection and processing of personal data. TSAs typically show data subjects a box outlining the data controller’s terms of service and requesting permission not only to collect the data but also to share it with other entities, or “third parties”. This is often referred to in short form as “notice and consent”. But these



notices don't provide any real agency to the data subject, who has no choice but to accept the agreement if they wish to use the service. In practice then, this situation gives users very little power over the processing of their data.

More personal data is being processed due to the popularisation of cheap, personal computers and digital devices, and the rise of data gathering by digital sensors and objects connected to the internet (often referred to as the internet of things). But that processing is also more revealing. With the growing digitisation of all aspects of human life, it's become possible to use personal data to build up a much more detailed and complex picture of individuals. Today, as well as the detailed personal information routinely collected by employers, health services, and government agencies, popular consumer technologies can reveal a person's exact movements on a given day, what they've bought, their online search history, and what they've 'liked' on social media. At the same time, advances in digital technologies mean that these diverse data sets can increasingly be compared and aggregated in meaningful ways.

The increasing amount of data being processed and the more sophisticated analysis of data has resulted in widespread benefits for individuals and societies; notably from more user-friendly consumer products and services, which now routinely customise themselves to users' specific tastes and needs. But it also means that the risks to human rights which inhere to data processing, discussed earlier in this chapter, are increasing. In this context, data protection regulation is meant to protect human rights, including the right to privacy, by giving individuals ability to control the processing of their data and imposing obligations on those who process the data.

There is general agreement that the ability for users to have adequate control of their personal data has become more difficult in the digital age and that there is a need to address that. But, as we'll see in the next chapter, there is significant disagreement about "what to do about it".







# CHAPTER II

# THE DEBATE





## The debate

The use of the internet and digital technologies have brought about social and economic benefits, to societies and individuals alike.

Individuals benefit from the ability to more connect more easily with people, and to both access and create new goods and services. But this has also created much more personal data, which is subject to processing, in turn creating more risks and potential harms if that data is not protected. Data protection aims to protect personal data from misuse and harm so as to ensure that the right to privacy is protected, while also protecting the ability to process data for economic and social purposes.

Due to the challenges associated with the digital age, most agree that there is a need to do more to ensure that this balance can be effectively respected. What they don't agree on is how this can be done.

## DIFFERENT APPROACHES TO SOLVING THE PROBLEM

A number of proposed solutions have emerged in recent years. Most of them include or build on measures rooted in existing data protection regulation. However, they differ when it comes to the amount of regulatory intervention they see as necessary for these measures to effectively work

One approach is broadly illustrated by the General Data Protection Regulation (GDPR), adopted by the European Union in 2016. The GDPR introduces a range of legally enforceable measures which build upon existing data protection regulation - including expanding user rights, increasing legal obligations on data controllers, and introducing an expanded definition of personal data.



Those who support the approach put forward by the GDPR argue that legally enforceable measures are necessary to tackle the challenges to the right to privacy posed by personal data processing in the digital age. Only these measures, they say, can provide sufficient protection. Non-regulatory measures, like awareness-raising campaigns for users, or investment in and promotion of privacy-respecting technologies, may be seen as useful or even necessary, but not as sufficient to ensure the right to privacy is respected in the digital age. Supporters of this approach argue that ensuring the right to privacy is respected through stronger regulation doesn't diminish the economic and social benefits of data processing, and might even enhance them – for example, by reducing the risk of data breaches and reputational damage for businesses.

This approach is generally favoured in countries where data protection regimes are comprehensive (see p.21), because there is already acceptance of the need for the broad application of data protection.

The comprehensive, regulatory approach to data protection is widely regarded as being the most human rights-respecting approach to data protection in the digital age. In chapter 4, we explore in more detail what a human rights-respecting data protection regime looks like.

However, this approach has attracted opposition from some quarters, who argue that a focus on regulation tilts the balance too far in one direction. Some highlight the economic losses that tighter restrictions on data processing – for example, measures to allow users to minimise or block access to their personal data while still using online services – might incur. They also point to the increased costs incurred by complying with such obligations.

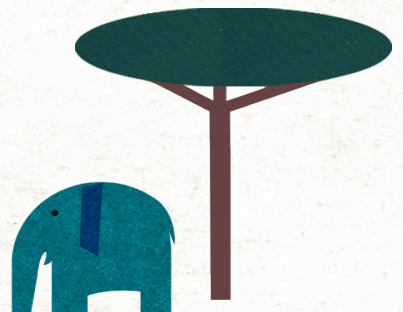
Others take issue with proposals to enable users to request deletion of personal data, arguing that this could undermine the rights to freedom of expression and access to information. And some, particularly in the open data community, fear these measures could limit the use of data to improve, and foster



innovation in, social and public services like transport systems, education, and healthcare.

Those who prefer to keep the status quo prefer to rely on “self-regulation”, which, in this context, means data controllers voluntarily choosing to implement measures to protect data. Under a self-regulatory approach, data controllers may be encouraged by relevant public authorities (through best practice guidance, for example) to simplify their terms of service agreements or to give more choice to users about how much of their data is collected; with additional measures like awareness-raising campaigns to encourage users to adopt privacy-respecting practices in their use of technologies.

This approach is often found in countries where data protection regimes are sectoral (see p.21), as well as in countries where private sector actors are not subject to data protection regulation.





## THE FACEBOOK–CAMBRIDGE ANALYTICA INCIDENT

In March 2018, media revealed that a British consulting firm, Cambridge Analytica, had acquired the personal data of 87 million Facebook users. Cambridge Analytica had already been in the public spotlight due to the company's role in providing data-driven consulting services to multiple candidates in the US presidential campaign.

The revelations in 2018 showed that Cambridge Analytica had used a personality quiz app which, in accordance with Facebook's own rules at the time, accessed the personal data available in their profiles. This included the work histories, birthdays, interests and hobbies, and events calendars not only of the app's users – which numbered 300,000 – but of their friends and contacts on Facebook, yielding personal data on 87 million people.

In 2015, Facebook became aware that Cambridge Analytica had acquired this data and received assurances that the firm would delete the improperly acquired data. However, the users whose data was implicated were not notified of this breach of Facebook's rules and Cambridge Analytica did not delete the data.

The revelations had global reverberations, with United States, Indonesia, India, the United Kingdom, and Brazil all expressing concerns that improperly acquired personal data could have been used by Cambridge Analytica or other political consultancies to influence elections or other democratic processes.

For many commentators, the story highlighted the limited role that consent plays in restricting data controllers' actions. Cambridge Analytica acquired

its data on the basis of the consent of the individuals who used the app. Whether those individuals knew the extent of what they were consenting to is a real question, but the situation demonstrates that sometimes internet users are willing to trade their personal data, and that of their friends and family, for access to online services, particularly when faced with an "all or nothing" choice, in which they cannot refuse access to data and still use the service.

The incident prompted a range of reactions from across a wide spectrum. Some saw it as illustrative of the need for stronger and data protection regulation; with US privacy advocates, media commentators and their British equivalents calling for tighter regulation and a comprehensive law. Even Facebook CEO Mark Zuckerberg admitted the company could be subject to further regulation.

However, some fear Facebook's revised privacy rules, by restricting the access of third parties to data generated by Facebook users, would also lock out researchers and academics who rely on access to data for social science research, including research into the use of social media and how it impacts individuals and society. An open letter published by academics and researchers expressed concern that the privacy changes would only increase Facebook's power to define a research agenda consistent with its own interests and would undermine independent oversight of how the platform functions and impacts its users.



## THE DEBATE IN THE REAL WORLD

### Controlling the collection of data

To understand how debates around data protection are playing out in the real world, it's instructive to look at what's happening around the first stage of the data processing cycle: collection.

Here, the divergence in approaches to regulation – outlined earlier in this chapter – is immediately apparent. On the one side, those who favour expanding regulatory measures argue that users should be provided with rights to choose specifically what data is collected about them and what uses this is put to, and to refuse to provide data that is not essential to using a service. They argue that, for example, users should be able to opt out of behavioural tracking for advertising purposes while using an app or service. Some comprehensive data protection regimes restrict data collection in this way by requiring companies to get informed consent from individuals before collecting their data, and ensuring that consent is tied to a specific purpose that is necessary for the provision of the service. Under this type of regulation, individuals shouldn't be asked to provide data that isn't necessary for that service.

On the other side, companies which rely on collecting or selling data about user behaviour argue that regulations which give users the right to minimise personal data while still using a service will erode the value of targeted advertising, which is the main revenue source for publishers online. These actors maintain that the provision of personal data for advertising purposes is part of the “value exchange” of the internet, whereby individuals can access essential search tools or social media sites entirely for free. Instead, they argue that publishers will be forced to compensate for this loss of revenue, perhaps by introducing fee-subscriptions or paywalls to access content and services.



## The right to be forgotten

Another prominent dimension of debates around data protection relates to the so-called “right to be forgotten” or “right to erasure.” This right, designed to enable individuals to ask companies to delete their personal data under certain conditions, has been criticised by some as threatening the right to freedom of expression and access to information. If broadly interpreted, some argue, it could lead to the restriction of free flow of information in a way that would harm the right to freedom of expression. However, others argue that having the right to be able to control what information is publicly available to others is a key component of the right to privacy. This debate is explored in more detail in chapter 3.

## Global level regulation

While most actors in the debate agree that there should be greater harmonisation of data protection frameworks across the world, the question of the level and types of regulation that data should be subject to remains contentious. Regulation, for example, via the form of a treaty, would set out minimum standards of data protection that would be legally binding on all states. Those who support a treaty argue that this is necessary because personal data receives different levels of protection according to the jurisdiction in which it’s processed. They also argue this would bring greater clarity for data controllers, who currently face a confusing array of different obligations, depending on the jurisdiction.

On the other hand, others argue that this approach would reduce data flows across borders because it would become too costly for some actors to comply with these obligations to use data. Instead, they argue for the strengthening of existing measures, like agreements negotiated between jurisdictions that regulate the transfer of personal data for processing across borders, contracts directly between data controllers across borders, and voluntary networks of data protection authorities that share best practices.



## STAKEHOLDERS

We've staked out the broad arguments in the data protection debate. Now we need to look at the participants in the debate – the stakeholders. Where do they sit on the question of how, and to what extent, the processing of personal data should be regulated?

### State

The state refers to the branches of an internationally recognised nation or territory and includes government departments, regulators, security and law enforcement agencies, and other public bodies. It is states which pass and enforce data protection legislation. However, states are made up of a number of bodies, all of which will have different priorities and perspectives on data protection. For example, in many countries, including those which have comprehensive data protection regimes, an independent public agency, or data protection authority (DPA), will be responsible for supervising compliance with any data protection legislation. These authorities are generally mandated to provide guidance on national data protection legislation and take enforcement action when the law is breached. They need to be well-resourced enough to carry out their functions and will have an interest in promoting strong privacy protections. However, states will also want to protect the ability to trade with other countries. For example, ministries of trade or those responsible for economic growth or investment may be interested in ensuring the free flow of data and not restricting the processing of data in a way that will burden trade and business interests.

Law enforcement agencies often face challenges in accessing data outside their jurisdiction during the course of criminal investigations due to different data protection legal frameworks which protect the right to privacy. They may, in some cases,



favour approaches to access to data which allow them to compel data controllers in other countries to provide data directly to them, instead of having to direct these requests to state bodies.

Data protection authorities are themselves a part of the state. As regulators charged with overseeing and enforcing data protection regulation, they will want to be sufficiently independent of other state bodies and be equipped with the powers to effectively implement data protection regulation.

## Users

Data protection was developed to protect users' rights and to correct the imbalance of power between users and those collecting data. However, users are not a homogenous constituency.

Some users might, for various reasons, take a greater interest in their privacy than others – whether because they are part of a technical community, or face particular risks to their security as an activist, human rights defender or member of a minority facing state harassment. As a result, they may take more concrete steps to protect their privacy, for example by employing specific technological measures to protect their data and minimise its collection.

Other users may prioritise the open access to information and convenience that the current business model of the internet provides, and see features like targeted advertising as an acceptable compromise. Some may even find these features useful and welcome them. Others may find them an excessive intrusion on their privacy and an unacceptable compromise for the use of services. While acknowledging this spectrum, it is probably safe to say that the majority of users will be interested in being able to use internet services and platforms at low cost, with minimum inconvenience, and minimum need to sacrifice control over their personal data and privacy.



## Civil society

Because data protection provides protection against abuses of rights and safeguards for individuals, civil society organisations tend to have an interest in regulatory approaches or comprehensive data protection regimes. However, civil society also includes groups that can rely on access to data to improve services for their beneficiaries, such as humanitarian and aid workers. Such organisations may also rely on direct marketing as part of their fundraising efforts, a practice that is impacted by stronger regulation. Therefore, stronger regulation may impose financial burdens on these organisations. Civil society also includes researchers and academics who may benefit from the use of **open data** or large data-sets (**big data**) which include or rely on personal data, and may therefore favour self-regulatory measures.

## Private sector

Stronger data protection legislation often imposes greater financial obligations on private sector actors that process data. At the same time, regulations which minimise the ability of private sector actors to collect data can pose challenges for companies that rely on data processing or on the sale and transfer of personal data as the basis of their revenue. This is particularly true of the advertising industry and for publishers that rely on the collection of data and selling of data to advertisers to maintain profitability.

However, private sector companies that rely on the use of personal data to provide targeted services also have an interest in retaining the trust of their customers, which stronger privacy protections in services and products can enhance. Smaller companies may prefer to implement such measures and market their commitment to privacy voluntarily, as the cost of complying with legislation may disproportionately impact them.



One of the greatest challenges for all private sector companies that operate in more than one country is complying with different data protection frameworks and determining which jurisdictions apply in different cases (see chapter 3). They may not necessarily advocate for global level regulation or a treaty which would impose the same standards on all countries, but support a harmonisation of data protection legislation across countries through closer coordination between governments and regulators.









## CHAPTER III

# WHY IS DATA PROTECTION A HUMAN RIGHTS ISSUE?





## Why is data protection a human rights issue?

As we started to look at in chapter 1, the issue of data protection has strong links to one of our fundamental human rights – the right to privacy.

Data protection also has links to other human rights, including freedom of expression and non-discrimination, which we explore later in this chapter. However, data protection arose, first and foremost, in order to tackle the challenges and risks posed to the right to privacy by increased processing of personal data.

In recent decades, the ability to control the use of personal data has been recognised as an essential element of that right to privacy. The exponential growth in the processing of personal data – and the increased risks this has generated – has pushed data protection up the policy agenda. In some states, there have even been advancements towards the recognition of data protection as a distinct and separate human right.

But whether as an element of the right to privacy or as a distinct human right, strong and effective data protection also helps protect other human rights. In this chapter, we look more closely at why data protection is such an important aspect of the right to privacy and how poor data protection standards can put that and other rights at risk.

## THE RIGHT TO PRIVACY

### What is the right to privacy?

Exactly what privacy means – and therefore the scope of the right to privacy – is not an easy question to answer. The UN Special Rapporteur on the right to privacy, whose role, among other



things, is to raise awareness about privacy issues, said in his 2016 report to the UN Human Rights Council that the concept of privacy “is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind” but that “there is no binding and universally accepted definition of privacy”. Indeed, the ICCPR itself does not say anything about what privacy means, but simply that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy”.

UN Special Rapporteurs are independent experts elected by the members of the UN Human Rights Council with particular thematic mandates, such as freedom of expression, privacy, poverty, or migrants. They publish annual reports on the subject matter of their mandate and receive and respond to complaints from individuals on related human rights issues.

With no clear definition set out in international human rights law, it has been left to others to try to provide potential definitions of privacy or at least to conceptualise the concept. An 1890 essay by two American lawyers, Samuel Warren and Louis Brandeis, was one of the first attempts to articulate what a right to privacy should encompass and summarised it as the “right to be let alone”. This, and other early attempts to define privacy, focused on the physical or territorial dimension of privacy, like bodily integrity and autonomy, and privacy of the home and correspondence.



## The role of international human rights law

The foundation of modern international human rights law is a document called the Universal Declaration of Human Rights (UDHR) which was adopted by the UN General Assembly in 1948. This was the first ever internationally-agreed document setting out the fundamental human rights of all people. The UDHR is not a treaty and so is not binding on states, but its provisions have acquired the status of customary international law and form part of enforceable international law. In any event, a number of international human rights treaties developed since the UDHR are binding on those states which have ratified them. On the issue of data protection, the most important of these is the International Covenant on Civil and Political Rights (ICCPR), which was adopted in 1966 and which guarantees the right to privacy.

As well as international treaties, many regional organisations have adopted their own human rights treaties, such as the European Convention on Human Rights, the American Declaration of the Rights and Duties of Man, and the African Charter on Human and Peoples' Rights.

Over the 20<sup>th</sup> century, there was increasing recognition of the importance of personal information as a further aspect of an individual's privacy. In 1967, Alan Westin, a leading academic expert on privacy, said that "[p]rivacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Just as privacy was recognised to include the ability to have autonomy over one's body, relations with others, and communications, so it became recognised as also including autonomy over information about oneself.



Rather than try to define privacy, others have taken a different approach. In 2006, Daniel Solove, another leading academic expert on privacy, proposed a taxonomy of privacy with four categories of activities which potentially harm privacy: information collection, information processing, information dissemination, and invasions. The first three of these all involve information about an individual: how it is collected (such as through surveillance), how it is stored and used (such as aggregating information from different datasets or weak security measures which result in risks of leaks and hacks), and how it is disseminated (such as its disclosure without the individual's consent), all of which relate to the different stages of data processing identified in chapter 1.

The approach of the UN Human Rights Committee has also been to look at categories of activities which impact upon privacy rather than trying to provide a comprehensive definition. In its General Comment on the right to privacy in 1988, rather than define privacy, the Committee set out a number of examples of what is covered within the scope of privacy. This included surveillance, searches of home and property, and personal and body searches. This General Comment also marked the first time that the Committee recognised personal information as an aspect of the right to privacy, saying that, "[t]he 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".

Established in 1977, the UN Human Rights Committee is a UN body made up of 18 independent experts on human rights, tasked with overseeing the implementation of the International Covenant on Civil and Political Rights. Among other things, the Committee issues General Comments which elaborate on different rights within the ICCPR and how they should be implemented by states.



## DATA PROTECTION AND PRIVACY

Despite the lack of any single, universally agreed definition of privacy, there is clear recognition and acceptance that the concept includes information about oneself and, in particular, the ability to control who has access to that information and how it is used.

In terms of personal information in the offline world, this is fairly straightforward. We can simply decide what information about ourselves we tell other people. But the advent of computers, the internet, and digital technologies more generally means that vast amounts of personal information are now collected by states, private sector organisations, and other actors. Many of the different types of personal information that are collected – and the ways they are used – are discussed in chapter 1.

### What the courts have said

In 1997, the European Court of Human Rights said that “the protection of personal data (...) is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life”. (*Z. v. Finland* (1997)) We can look at a couple of real life examples to see how the misuse of personal information can lead to clear violations of the right to privacy:

- In the case of *Biriuk v. Lithuania* (2008), the applicant was a woman living with HIV who lived in the village of Kraštų. The fact that she was HIV-positive was published in a local newspaper after a local hospital confirmed the fact to the newspaper without the applicant’s knowledge or consent. The European Court of Human Rights found that this was a clear case of a breach of the woman’s right to privacy, an “outrageous abuse of press freedom” and that misuse of her personal information had caused her public humiliation and exclusion from local social life.



- In the case of *Rotaru v. Romania* (2000), the applicant was a Romanian national who had been persecuted and imprisoned in the 1940s by the communist regime for protesting restrictions on freedom of expression. In the 1990s, during unrelated court proceedings, the Ministry of Interior submitted as evidence to the court a letter it had received from the Romanian Intelligence Service in which it was said that they had a file on the applicant stating that he was a member of a legionnaire movement in the 1940s, as well as a number of other pieces of information about him. The applicant argued that this and the other assertions in the letter were false and defamatory but, despite bringing proceedings against the Intelligence Service, was unable to obtain a copy of the file or have the false information corrected or deleted. The European Court of Human Rights held that this information constituted “personal information” which was protected under the right to privacy, that it could injure the applicant’s reputation, and that the failure of Romanian law to allow him to access and, if necessary, have the false information corrected or deleted was a breach of that right to privacy.

Data protection, as we also saw in chapters 1 and 2, is the regulation of the collection, storage, use, and dissemination of personal information once it has been volunteered by an individual or obtained in some other way. It is therefore the means by which information is protected from unauthorised access or use. In essence, data protection offers a means of ensuring that individuals retain autonomy over information relating to themselves, securing their right to privacy.

CC BY-NC-ND 4.0 International license



## A right to data protection?

Although it is well-established that data protection is an aspect of the right to privacy, some jurisdictions now consider data protection to be a human right in and of itself.

The Charter of Fundamental Rights of the European Union, which was adopted in 2000, and became legally binding in the EU in 2009, is the first example of an international human rights instrument containing a standalone right to data protection. Article 8 provides that “everyone has the right to the protection of personal data concerning him or her”. It also requires that 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” and guarantees that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified”. Finally, it also requires that EU member states designate an independent authority to ensure compliance with these rules.

As well as the EU, there are a small number of states which recognise a right to data protection as a standalone right in their own national legal systems. The constitutions of Angola, Colombia, Croatia, Greece, Portugal, Slovenia, and Turkey, for example, all contain, in some form, a right to data protection.

The 2012 Association of Southeast Asian Nations (ASEAN) Human Rights Declaration also makes specific reference to data protection, noting that “every person has the right to be free from arbitrary interference with his or her privacy, family, home, or correspondence including personal data (...).”



### The balancing act

Although there is no definitive list of factors that should be considered when balancing the rights to privacy and freedom of expression in cases involving personal data, some courts have set out relevant considerations. In *Von Hannover v. Germany* (No. 2) (2012), this balancing act was undertaken by the European Court of Human Rights. The case was brought by Princess Caroline and Prince Ernst August von Hannover, photos of whom had been published without their consent in German magazines. They argued that this constituted a breach of their right to privacy. In balancing their right to privacy against the right of the magazines to freedom of expression, the court laid down the following factors to consider:

- The contribution that the publication makes to a debate of “general interest” (the court suggested political issues, crimes, sporting issues, and performing artists would be issues of such general interest, but that the marital or financial difficulties of a person would not be);
- How well-known the persons concerned are (with a distinction made between private individuals and persons acting in a public context on the one hand, and public figures on the other);
- The prior conduct of the persons concerned (previous cooperation with the media, for example, limiting a person's ability to argue that their privacy had been breached);
- The content, form, and consequences of the publication (with factors such as the size of a publication's readership being relevant); and
- The circumstances in which the information (in this case, photos) was obtained (with relevant factors including whether the person gave their consent or whether it was done without their knowledge or by illicit means, the nature and seriousness of any intrusion, and the consequences for the person involved).

Examining the case in question against these factors, the court found that there had been no violation of the Von Hannovers' rights to privacy.



## DATA PROTECTION AND OTHER HUMAN RIGHTS

All human rights are universal, indivisible, interdependent, and interrelated. Adverse impacts upon one right will often also impact negatively upon the exercise of other rights, and the facilitation of one right will often further enable the exercise of others. This is certainly the case when it comes to the issue of data protection which, as we have seen, is closely connected to the right to privacy.

- **Right to non-discrimination:** The right to non-discrimination is protected under Article 7 of the UDHR and Article 26 of the ICCPR, as well as in regional human rights instruments. Information about an individual may directly or indirectly reveal their personal characteristics - characteristics which they may not wish others to know or which could result in discrimination. In particular, the ability not to reveal characteristics which may be invisible, such as religion, sexual orientation, gender identity, or health status may be fundamental to ensuring protection from discrimination. Strong data protection therefore ensures that the individual remains in control of information which could result in discrimination were it to be known by a third party. Conversely, unauthorised access to an individual's personal data may – as well as constituting a breach of the right to privacy – result in discrimination.

It is not just the existence of personal data that may result in discrimination, but also its processing, particularly where individuals are profiled on the basis of their personal data.

**Profiling** can be used by state actors and private companies to make decisions which affect how a person is treated, what services they are offered and under what conditions. There is therefore a risk that a person could face discrimination if, as a result of profiling, they received less favourable treatment due to possession of a particular characteristic which cannot



be justified. This may happen if the **algorithms** developed for profiling incorporate the conscious or unconscious biases that exist offline.

One example that has been evidenced is the use of algorithms in the US to make risk assessments on whether a person charged with a criminal offence should be released on bail. The algorithms use police data, such as the number of re-arrests of people for the same offence, to create the risk assessment. However, as re-arrests by police officers may have been due to racial discrimination, the algorithms have led to certain ethnic minority groups being less likely to be released on bail than others. Recent pieces of data protection legislation have sought to mitigate this particular risk: the EU's GDPR, for example, gives all data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects them or produces legal effects concerning them.

- **Right to freedom of expression:** The right to freedom of opinion and expression is protected under Article 19 of the UDHR and Article 19 of the ICCPR, as well as in regional human rights instruments. The right includes the freedom to seek, receive, and impart information, ideas, and opinions, regardless of frontiers and in any form. The ability to remain anonymous when expressing certain forms of speech, opinions, or other expression can, in some circumstances, be critical. In societies where certain statements can lead to retribution or persecution, sometimes individuals can only express themselves freely under the cloak of anonymity, which the internet in particular allows. In many parts of the world this ability is being undermined. At least 49 African countries require individuals to register their personal information with network providers before they activate a SIM card, leading to the creation of extensive databases of user information, and eradicating the potential for any anonymity of online communications. In 2013, the UN Special Rapporteur on the promotion and protection



of the right to freedom of opinion and expression expressed his concerns at this development, noting that it was often a lack of data protection legislation that enabled governments to cross-reference SIM users' information with other private and public databases, and build detailed profiles of individuals.

## HUMAN RIGHTS IN CONFLICT?

While strong data protection is essential to the enjoyment of the right to privacy, limiting the availability of personal data can, in some circumstances, come into conflict with other human rights, particularly the right to freedom of expression. If the right to freedom of expression means the right “to seek, receive and impart information and ideas of all kinds” (the language used in Article 19 of the ICCPR), then any prohibition on the ability to access, use, or publish public information – because it is personal data – will constitute an interference with this right.

However, just as the right to privacy is not an absolute right, the right to freedom of expression is not an absolute right either. Restrictions are permissible in certain circumstances, known as exceptions. However, in order for these to be human rights-respecting, they have to meet certain tests. There must be a legal basis for the restriction, it must be in pursuance of a legitimate aim, and it must be proportionate. These tests are outlined in greater detail in annex 2 (pp. 92-3).

Some data protection frameworks contain specific exemptions in order to protect other aspects of the right to freedom of expression. The OECD Privacy Guidelines, for example, say that they “should not be interpreted (...) in a manner which unduly limits the freedom of expression” (Principle 3(b)) and the EU GDPR allows member states to have exemptions in national law in order to “reconcile the right to the protection of personal data (...) with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression”.



### “The right to erasure” or “the right to be forgotten”

One issue which has pitted the rights to privacy (and data protection) squarely against the right to freedom of expression is the so called “right to be forgotten” or “right to erasure” which now exists in a number of jurisdictions. The concept was first developed by the European Court of Justice in 2014 when interpreting the EU’s Data Protection Directive 95/46 (since superseded by the GDPR). The court held that an individual could request a search engine to have links to certain web pages “deindexed” from their name, meaning that search queries containing their name would not return those web pages as part of the search results. To do this, individuals would have to establish that those web pages contained information about them that was “inadequate, irrelevant or no longer relevant”.

That right has been further elaborated in the “right to erasure” provision in Article 17 of the GDPR, which expands its scope to include a right to make such a request to any data controller and for the data to be erased in its entirety. Where individuals make a request for the erasure of personal data, the data controller must then erase that data under certain circumstances (e.g., if the data is no longer necessary, if the individual withdraws their consent for processing, or if the data is being processed by an online service or platform) unless one of the listed exceptions applies, such as in cases where information is necessary “for exercising the right of freedom of expression and information”. A similar provision, with narrower exceptions, can be found in Article 43 of the Constitution of Argentina.

Some argue that the right to erasure is necessary if individuals are to have meaningful control over information which relates to them, something which, as we’ve seen above, is an aspect of their right to privacy. Others argue that the global removal of information about an individual simply on the basis that they don’t want it to be there represents a threat to the right to freedom of expression, with important information in the public interest at risk of being erased.







CHAPTER IV

# WHAT WOULD A HUMAN RIGHTS-RESPECTING DATA PROTECTION REGIME LOOK LIKE?





## What would a human rights-respecting data protection regime look like?

As we saw in chapter 1, the concept of **data protection** arose in the 1960s in response to concerns that the rapid increase in the processing of **personal data** could lead to violations of individuals' right to privacy.

In order to address these concerns, a set of guiding principles were developed to ensure that personal data could be processed without violating human rights. By the early 1980s, these principles had been codified in two international texts which are explained in more detail below.

These principles, once implemented into national law, impose obligations on **data controllers** and provide rights for users in relation to the processing of their data. Therefore, data protection and human rights (particularly the right to privacy) have always been inextricable. These principles underpin data protection frameworks across the world, whether those frameworks are binding (such as legislation) or non-binding (such as voluntary frameworks or guidelines).

But when it comes to data protection, it is not only the content of any one law or policy which determines whether a country has a data protection regime which is human rights-respecting. As we saw in chapter 1, a data protection regime can either be comprehensive, which means that legislation applies to the private and public sector, or it can be sectoral, which means it only applies to some sectors.

There are four key elements which determine whether a country has a human rights respecting human rights regime:



- 1) the existence of a data protection law;
- 2) the incorporation of internationally agreed minimum data protection standards in the law;
- 3) the extent of the coverage of the data protection law; and
- 4) the existence of an enforcement, or regulatory, authority.

Only if a country has all four elements in place can it be deemed to be human rights-respecting. Below we consider each element in the form of key guiding questions which can be applied to any country.

## 1. Does a data protection law exist?

Passing a law on data protection is the first step a state can take towards a rights-respecting data protection regime.

But here an obvious question arises. Does a state have any obligation even to take this first step?

The answer is yes. When it comes to the protection of human rights, states have both negative and positive obligations.

- Negative obligations are about refraining from taking actions which adversely impact upon human rights.
- Positive obligations require the state to take certain steps to ensure the protection of human rights.

In the case of data protection, it is this positive obligation which is particularly important. As we have seen in chapter 3, personal data and its collection, storage, use, and dissemination all impact upon a person's right to privacy and potentially put it at risk. States therefore have a positive obligation to take steps to ensure that individuals' right to privacy is protected, and establish accountability and liability if it is breached.

The Human Rights Committee's General Comment on the right to privacy is clear that it should be legislation – as opposed to some other measure – which sets out who has access to information concerning a person's private life, as well as how it can be processed and used.



## 2. Does the data protection law incorporate the minimum standards needed to ensure that an individual's right to privacy is protected?

Data protection legislation should be consistent with the international standards that have been established. While international human rights law itself does not provide specific detail on what rights-respecting legislation should look like, this gap has been filled by the two texts below.

- **OECD guidelines on privacy and transborder data flows:**  
The OECD is an intergovernmental organisation of 35 high-income economies founded to stimulate economic progress and world trade. In 1980, it developed a set of privacy guidelines to harmonise rules around, and minimise barriers to, transborder flows of personal data, which were increasing rapidly at the time. The guidelines were updated in 2013.
- **Convention 108:** The Council of Europe is an intergovernmental organisation made up of 47 European countries. Its stated aim is to uphold human rights, democracy, and rule of law. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (or “Convention 108” for short) was adopted in 1981 and has been ratified by all 47 member states of the Council of Europe. It is also open to ratification by states who are not members of the Council and is the world's only legally binding instrument specifically focused on data protection.

Though there are some small differences, there is a great deal of overlap between the two sets of standards. We outline what those standards are on the next page. As noted above, the standards contained within the OECD Privacy Guidelines and Convention 108 are the minimum required for an individual's right to privacy to be protected. However, there are an increasing number of instances in which states have provided stronger protection for individuals' right to privacy in data protection legislation, most notably the member states of the EU through the GDPR (see box on pp. 56-7).



## The ten minimum standards

- 1. Fairness and lawfulness:** Personal data should be collected (and thereafter stored and used) fairly and with the consent of the **data subject**, or on some other legal basis.
- 2. Data quality:** Personal data should be adequate, relevant and not excessive in relation to the purposes for which it is stored and used.
- 3. Purpose specification:** Personal data should be collected, stored and used for legitimate purposes only, and not in a way which is incompatible with those purposes.
- 4. Notice of purpose:** The data subject should be informed of the purposes for which their data is being collected, stored and used at or before the time of its collection.
- 5. Limited use:** Personal data should not be used or disseminated for purposes other than those specified at the time of its collection, except with the consent of the data subject or by the authority of law.
- 6. Security:** As a result of the risks to an individual's privacy that might arise if their personal data was lost, stolen, or leaked, data protection legislation should require data controllers to take appropriate security measures.
- 7. Openness:** Given that personal data relating to individuals may be collected without their knowledge, data protection legislation should require a body – whether a public authority, a private business or other – to inform individuals when it collects personal data about them.
- 8. Access:** Individuals should also be able to request, without excessive delay or expense, any personal data which has been collected on them, in an intelligible form.
- 9. Correction or deletion:** An individual should be able to correct or delete any data which is inaccurate or which was processed contrary to the above principles.
- 10. Accountability, sanctions, and remedies:** Data controllers should be accountable for complying with the requirements of the data protection legislation.



Because the right to privacy is not an absolute right and must be balanced with others, including the right to freedom of expression, it is important that data protection laws also allow for exceptions. However, in order for these exceptions to be human rights-respecting they must meet certain tests, i.e. they may only be permitted where there is a legal basis for the restriction, where it is in pursuance of a legitimate aim, and where it is proportionate. These tests are outlined in greater detail in Annex 2 (see pp. 92-4).

### Beyond the minimum standards: the EU's GDPR

The GDPR builds on the existing standards by extending the definition of personal data, providing users with more rights to control the processing of their data and imposing more obligations on data controllers with regards to the processing of personal data.

Below are some examples of how the GDPR builds on and extends the minimum standards:

- **Consent:** The minimum standards generally require the consent of the data subject before personal data can be collected (or stored, used or disseminated), but do not specify what “consent” means. In practice, as was noted in chapter 1, data subjects often “consent” by ticking a box at the end of long, technical, and complicated terms of service agreements. The GDPR attempts to make consent more informed by requiring any written request for consent to be in “an intelligible and easily accessible form, using clear and plain language”.
- **Broader definition of special categories:** The GDPR contains a definition of “special categories” of personal data which is broader and more expansive than that of Convention 108. There are greater limits on personal data revealing a



person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation.

- **More rights for users to delete their data:** The minimum standards only give the data subject the right to have their personal data deleted where it is inaccurate, or where it was processed contrary to the other principles. The GDPR, however, also allows data subjects to request that personal data be deleted simply on the basis that they no longer consent to any future processing of that data and that there is no other legal basis for its processing, a provision known as “the right to erasure”. As noted in chapter 3, this could potentially conflict with other rights, particularly the right to freedom of expression, and so the GDPR contains an exception to the right to erasure where processing that personal data is “necessary for exercising the right of freedom of expression and information”.
- **A right to object to decisions made on automated processing:** The minimum standards do not say anything about the rights of data subjects when decisions are made through automation which concern them. The GDPR, gives data subjects the right not to be subject to a decision based solely on automated processing (including **profiling**) which produces legal effects concerning them or otherwise significantly affects them.
- **Reporting requirements for data breaches:** The minimum standards do not say anything about what a data controller should do in the event of a data breach. The GDPR states that where a data breach containing personal data takes place which is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the personal data breach to any affected data subjects without undue delay.



### 3. Is the data protection law comprehensive?

The right to privacy in Article 17 of the ICCPR makes no distinction between impacts on privacy stemming from actors in the public sector, private sector, or elsewhere, while the Human Rights Committee's General Comment on the right to privacy is equally clear that such data protection legislation must apply to *all* personal data, whether it is collected, stored or used by "public authorities or private individuals or bodies". This means comprehensive data protection legislation.

The requirement for comprehensive data protection legislation can also be found in two key international standards developed in Convention 108 and the OECD Privacy Guidelines. We'll look at these in more detail in the next chapter, but Convention 108 requires all states which have ratified it to "take the necessary measures in its domestic law" to give effect to its provisions, and the OECD Privacy Guidelines say that states should adopt "national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines".

While in theory states could comply with their obligation to develop and implement comprehensive data protection legislation by adopting several laws which regulate data protection in different areas of life, or different laws for different aspects of data protection, recognised best practice is to have a single piece of legislation with a consistent level of protection. There is no definitive list of which states have such data protection legislation, but it is a significant number. Professor Graham Greenleaf of the University of New South Wales, who monitors data protection legislation around the world, has estimated that as of 2017, 120 states had some form of comprehensive data protection legislation.



#### 4. Is there an enforcement authority with the powers to enforce the legislation?

As well as ensuring that there is data protection legislation regulating the collection, storage and processing of personal data, international standards also require the establishment of an enforcement authority. The authority should be empowered to enforce the data protection legislation, as well as conduct investigations or pursue enforcement proceedings where there has been a breach of that legislation. It should be independent of government but provided with sufficient resources to be able to exercise its powers effectively and make decisions on an objective, impartial, and consistent basis.









## CHAPTER V

# WHERE ARE DATA PROTECTION STANDARDS SET?





## Where are data protection standards set?

So far, we've talked about what data protection is, its relationship to human rights, and what makes a rights-respecting data protection regime.

In this chapter, we look at where data protection standards, both binding and non-binding, are made. Examples of binding standards include laws and regulation. Non-binding standards can be best practice guidelines or voluntary frameworks. Both non-binding and binding standards are developed at the national, regional or international levels.

Wherever you are, the most influential standards will be binding ones and will, in most cases, be passed at the national level. Only states and one supranational organisation (the European Union) have the ability to pass binding legislation within their particular jurisdiction. This is why it's particularly important for human rights defenders to engage at the national level with their governments, which we focus on in the first section of this chapter.

However, there are also regional and international level bodies which have set binding data protection standards in the form of treaties. Depending on a country's internal constitutional requirements, the treaty may require domestic legislation in order to have legal effect. However, because of their binding nature under international law on the states that have ratified them, we also look at them in this section.

Non-binding standards like guidelines or declarations can also have an important influence on norm-setting in the field of data protection. We indicate where human rights defenders may engage to influence these types of standards at the national, regional, and international levels later in the chapter.



## BINDING DATA PROTECTION STANDARDS

### National level

Depending on the state, data protection legislation may be made by the legislature, government, or other state bodies, and it will take one of two general forms:

- **Comprehensive:** If a country has “comprehensive data protection” it means that the legislation applies to data processed by any entity in that country, whether it is public or private, regardless of sector. This is true of more than 100 countries as of 2018.
- **Sectoral:** In some countries, regulation only applies to data processed by the public or private sector. In other countries, regulation only applies to particular fields or industries within the public or private sector that process data (e.g. healthcare or education). For example, in the US, which has a sectoral data protection regime, Congress (the legislature) has passed legislation which deals specifically with data protection but only applies to data held by government federal agencies (the Privacy Act of 1974 and the Computing Matching and Privacy Protection Act of 1988). There are also laws relating to specific types of personal data: the Children’s Online Privacy Protection Act of 1998, for example, and the Health Insurance Portability and Accountability Act of 1996. These laws, along with constitutional protection of the right to privacy, encompass data protection in the US.





### Should civil society engage?

Absolutely. As we saw in chapter 4, comprehensive data protection at the national level is the simplest route to a human rights-respecting data protection regime. For civil society in countries with no data protection or with limited or sectoral legislation, it's therefore important to push for comprehensive data protection. And in countries where comprehensive data protection exists, it's essential to ensure that the legislation is enforced and is updated where applicable to be in line with best practice, outlined in chapter 4. For tips on how to advocate at the national level in each of these scenarios, see chapter 6.

### European Union

The EU, as a supranational organisation, can pass legislation which is binding on its members. Some EU law is directly binding on member states, whereas some requires implementation by the member states via their own domestic legislation. Just as at the national level, this legal order is divided into primary legislation (treaties) and secondary legislation (based on treaties).

Primary legislation is provided for in a number of treaties including the two core treaties, the Treaty of the European Union and the Treaty on the Functioning of the European Union. These have been revised a number of times, most recently by the 2009 Lisbon Treaty, which also incorporated the Charter on Fundamental Rights. Through Article 8 of the Charter, the EU notably provides – in a high-level, core treaty text – not only a legal basis for data protection, but a right to the protection of personal data.

Secondary legislation comes primarily in the form of Directives



and Regulations, which are legislative acts and binding on EU member states. The most important piece of EU secondary legislation relating to data protection is the GDPR (Regulation (EU) 2016/679). This general Regulation is the most authoritative source of data protection standards at the EU level, but not the only one. Data protection standards will also continue to be set by other forms of secondary legislation complementing the GDPR, like the Directive on protecting personal data processed for the purpose of criminal law enforcement (2016/680), and the e-Privacy Regulation.

Compliance with the GDPR at the EU level is monitored and enforced by the European Data Protection Board (EDPB) and the European Court of Justice (the CJEU). The CJEU is the highest court in the EU and its interpretations of EU data protection legislation provide further guidance on data protection standards and how to ensure their equal application across all EU member states. Between 2001 and 2016 the court issued more than 40 decisions relating to data protection. The most significant of these are *Schrems v. Data Protection Commissioner* (2015), which struck down the bilateral US-EU “Safe Harbour” data sharing agreement, and *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos* (2014), which ruled that Google and other internet search engines must “delink” certain search results in order to remove personal data which is “inaccurate, inadequate, irrelevant or no longer relevant” from their search results at the request of users (more commonly known as “the right to be forgotten”).

Under the GDPR, the EDPB acts as an important source of data protection standards by virtue of its mandate to provide independent analysis of trends and compliance with the regulation, including via “Opinions” and “Recommendations” on data protection legislation and policy development.

Due to trade between EU and non-EU countries, and the requirement that businesses outside of the EU which process the personal data of individuals in EU countries abide by EU standards (the “adequacy” requirement), the GDPR impacts countries beyond the EU.



### Should civil society engage?

For human rights defenders based in countries which are members of the EU, enforcement of the EU's data protection framework is essential to ensuring that the standards it sets out are actually enforced. The GDPR also enables non-governmental organisations to take legal action on behalf of individuals – for example, by pursuing class-action litigation at the CJEU. Although litigation is expensive, it will have an important effect on the interpretation and enforcement of the data protection standards included in the GDPR.

Human rights defenders can also monitor data controllers and bring complaints relating to infringements of the GDPR to their national DPA, which has the authority to bring these complaints to the EDPB and, if necessary, the CJEU.

Future revisions of the GDPR and other components of the EU's data protection framework, such as the e-Privacy Regulation, will also be important opportunities for civil society to engage.

## International

### Council of Europe

The Council of Europe (CoE) was founded in 1949 and is an international organisation whose stated aim is to uphold human rights, democracy, and the rule of law in Europe. Unlike the EU (see above), the CoE does not have legislative powers. Instead, the Council functions to ensure agreement and compliance through treaties which harmonise or provide common legal standards for its members.



The CoE has played an important role in the shaping of the fundamental data protection standards and in their widespread adoption by issuing Convention 108 in 1981 (see chapter 4), which is the only multilateral, international legal instrument on data protection that is open to ratification by non-members of the Council.

In addition to Convention 108, the CoE's Convention on Cybercrime (also known as the Budapest Convention), an international treaty, also contains reference to data protection and cross-border access to data in its Article 32.

### Should civil society engage?

Yes. In 2018, Convention 108 underwent a modernisation which included measures to harmonise it with other instruments (like the GDPR), along with a new mechanism for enforcement and accountability, the Convention Committee. It is therefore essential that civil society from countries which are signatory to the Convention engage with the Committee to ensure effective implementation of the Convention at the national level.

For civil society in countries which are not signatory to the Convention, it is worth considering working with your government to pursue ratification of the treaty. The first step is for a government to be granted "observer" status and participate in the work of the Committee of the Convention which oversees its implementation. The Convention is being modernised to bring its standards into closer alignment with that of the EU.

In addition, the Council of Europe is updating the Budapest Convention by adopting an Additional Protocol. As this



protocol will address data protection safeguards, it is important that human rights defenders engage in its development and ensure it aligns with the data protection safeguards afforded in Convention 108.

For tips on advocacy messages which make the case for adopting strong data protection, see chapter 6.

### The African Union

The African Union (AU) is a regional body which comprises all 55 countries of the African continent. It is made up of an array of political and administrative bodies which are responsible for developing and implementing the decisions and commitments of the Assembly of the AU, which twice a year assembles the heads of state of its members.

In 2014, the Assembly adopted a Convention on Cybersecurity and Personal Data Protection, the aim of which is to spur the development of national and sub-regional frameworks for cybersecurity and data protection on the continent as well as ensure their harmonisation. It is based on the principles of the CoE's Budapest Convention, as well as the ten minimum standards of data protection found in the OECD guidelines and Council of Europe Convention 108 (see pp.54-5).

To date, only eight countries have signed the Convention and none have ratified it. As a result, it is yet to come into effect, and has had no discernible impact on data protection standards on the continent.



### Economic Community of West African states

The Economic Community of West African States (ECOWAS) is a sub-regional body made up of 15 member states in the West Africa region, primarily created to promote economic integration. In 2010 it adopted a legal instrument binding on all its members: the Supplementary Act on Data Protection. The Act draws on the EU 1995 Directive, specifies the principles and practices that data protection legislation should incorporate, and mandates the establishment of an independent supervisory authority to oversee compliance. Since its passage in 2010, the Act has led to the development of data protection legislation in seven ECOWAS member countries (as of 2018).

## NON-BINDING DATA PROTECTION STANDARDS

### National

Voluntary codes of conduct also play a role in how data is protected. These can take the form of “privacy seals”, trustmarks or certificates which can be issued by authorities or by other agencies to show commitment by data controllers and processors to compliance with data protection standards. The role that these instruments play in data protection standards depends on the regulatory culture and context of the country. For example, in the US, where there is more emphasis placed on the self-regulatory role of the markets than on regulation by the state, codes of conduct play a key role in data protection and are enforced by a consumer protection body, the Federal Trade Commission. In countries with comprehensive data protection legislation that applies to both the public and private sectors, codes of conduct will likely be both issued and supervised by the DPA.

Codes of conduct also play a role in supporting bilateral and cross-border flows of data. Under the GDPR (and its predecessor the Data Protection Directive), companies processing data relating to EU citizens can sign a code of conduct which allows them to transfer it to third parties.



## International

### Council of Europe

In addition to Convention 108 (see above), the Committee of Ministers and the Parliamentary Assembly have issued specific recommendations on a wide range of issues relating to data protection (such as Recommendations on the use of Personal Data for Employment Purposes, for Social Security Purposes, and for Statistical purposes) which can also be influential on members' policy development and the interpretation of existing laws and policies.

### Should civil society engage?

For human rights defenders, the most important avenue to ensure protection of human rights is through the adoption and enforcement of comprehensive data protection regimes, which imposes binding regulation on all sectors.

However, particularly in countries with sectoral data protection regimes, non-binding standards can be a helpful tool, and human rights defenders can monitor companies' compliance with voluntary trustmark or accreditation schemes in order to ensure accountability. This should be seen as complementary – rather than an alternative – to comprehensive data protection.

### Organization of American States

The Organization of American States (OAS) is a multilateral organisation founded to promote “regional solidarity and cooperation” among its member states, and is made up of 35 states in the Americas.

The OAS has so far taken limited action with regards to data protection, with the most significant step being a General



Assembly resolution in 2014, calling for a study on preliminary principles and recommendations on data protection. The resulting report was adopted in 2015 by the Inter-American Judicial Committee of the OAS. It takes the form of an analysis of the different approaches to data protection in Europe, in the US, and in states across Latin America, and provides a set of 15 legislative guidelines. These relate to **data processor** and **data controller** responsibilities in collecting and processing data, third party processors, and cross-border transfers, and recommend that OAS states create an independent supervisory authority to ensure enforcement.

### Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN) is a regional organisation made up of ten member states in the South East Asian region, governed by a charter. It was set up primarily to promote cross-border trade. In 2012 it adopted a Human Rights Declaration, which includes a reference to personal data (Article 21). However, the Declaration as a whole has been criticised by human rights defenders and the Office of the High Commissioner for Human Rights for not “complying with international standards”. Nevertheless, ASEAN has made commitments to promoting the adoption of data protection legislative frameworks via the e-ASEAN Framework Agreement (2010), mainly to promote e-commerce. So far, ASEAN has not developed an organisation-wide commitment or standards on data protection.

### Asia Pacific Economic Cooperation

Asia Pacific Economic Cooperation (APEC) is a high-level regional forum which was founded in 1989 to promote free trade throughout the Asia-Pacific region. It convenes the heads of state of its 21 member states once a year, issues declarations and guidelines, and makes recommendations to states in order to



promote trade and cross-border cooperation. Unlike other similar bodies, it does not have a founding treaty or constitution, and instead operates on the basis of consensus. Its outcomes therefore do not have any legal or binding value, and rather represent a general commitment to work together towards shared goals.

In 2003, APEC's Electronic Commerce Steering Group developed a "Privacy Framework", based on the OECD Privacy Guidelines, which was adopted by the member states in 2004. However, it has been criticised for representing a watered down version of the original OECD guidelines, particularly through its emphasis on "choice" (and concurrently reduced obligations on data controllers) and its weak protections for individuals whose data is exported to a third party overseas. The APEC Privacy Framework imposes no obligations on the exporter or importer of data to another jurisdiction, nor contains provisions for enforceability or accountability. Nevertheless, data protection laws in a number of Asian states contain stronger provisions than those found in the framework, often as a result of a desire to comply with European adequacy requirements for cross-border data transfers.

### The African Union

In order to facilitate greater uptake and implementation of the AU Convention on Cybersecurity and Personal Data Protection, the AU Commission, together with non-governmental organisation the Internet Society, launched a guidance document on data protection, the Personal Data Protection Guidelines for Africa. The guidelines provide recommendations for a range of stakeholders on developing policies and regulation on data protection.

### East African Community

The East African Community (EAC) is a sub-regional body made up of six member states. Its aim is to promote cross-border trade between these countries and, as with other regional economic



communities, it has established a common market for trade in goods, labour, and capital. Within this mandate, it adopts frameworks, and agreements to encourage harmonisation of laws and regulations and promote growth and trade. In 2010, it adopted a Framework for Cyberlaws which includes provisions on data protection and privacy. To date, four out of the six member states have developed draft legislation on data protection.

### **The United Nations Security Council**

The UN Security Council is charged with the maintenance of international peace and security among UN member states and is made up of representatives of fifteen states. The resolutions it issues are binding on all UN member states. Although the Security Council has not issued any resolutions on data protection, they have made reference to data protection in resolutions on counter-terrorism and anti-money laundering measures.

### **UN General Assembly**

The UN General Assembly (UNGA) played an early role in the development of data protection standards. In 1976, it issued a report which called for the development of international standards relating to the rights of the individual against threats from the use of computerised data systems, and urged member states to adopt appropriate legislation to protect personal data.

This led to UNGA's adoption in 1990 of the UN Guidelines for the Regulation of Computerized Personal Data Files, a document which includes the basic data protection principles set out in the OECD Privacy Guidelines and Convention 108 (see chapter 4). However, aside from reiterating general agreement on these basic data protection principles, the UNGA has arguably had less influence in the takeup of data protection laws than the OECD Privacy Guidelines and the CoE Convention 108.



### UN Human Rights Committee

The Human Rights Committee can issue General Comments that elaborate on the meaning of particular human rights contained in treaties. These do not have binding force but can constitute useful guidelines for states on how to implement rights contained in the treaties. The 1988 General Comment on Article 17 of the ICCPR, for example, notes “the gathering and holding of personal information on computers, databanks, and other devices whether by public authorities or private individuals or bodies, must be regulated by law (...) Effective measures have to be taken by states to ensure that information concerning a person’s private life does not reach the hands of persons who are not authorised by law to receive, process and use it (...)”.

### UN Human Rights Council

The UN Human Rights Council (UNHRC) has adopted resolutions (in 2013, 2014 and 2016) on the right to privacy in the digital age which make explicit reference to data protection. The 2016 resolution, for example calls on states “to develop or maintain and implement adequate legislation with effective sanctions and remedies that protect individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data”.

### The World Trade Organisation

Ensuring that data can flow across borders in order to promote trade and commerce has been one of the main imperatives behind the development of data protection legislation and international agreements, as discussed in chapter 2. The most important global trade agreement is the General Agreement on Tariffs and Trade (GATT), overseen by the World Trade Organisation (WTO). The GATT is a legal agreement between member countries of the



WTO, making them legally bound to measures that protect trade liberalisation (such as the elimination or reduction of tariffs or taxes on the import and export of goods and services). One provision in the GATT which could be seen as a potential challenge to certain data protection principles (like the EU's "adequacy" principle) and could serve to weaken data protection and standards is a proviso referring to the "disguised restriction on trade in services".

### The Group of 20

The Group of 20 (G20) is a group of nineteen of the world's largest economies and the EU, which meets once a year at the G20 Leaders' Summit, where each member is represented by a high-level representative such as the head of state. The host country or "presidency", of the G20 rotates every year and decides the annual agenda of the meeting on a wide range of issues relating to the global economy. The meeting results in the adoption of a Leaders' Declaration, which presents agreed positions on issues on the agenda. Although not binding, this declaration can include commitments by member states and can therefore act as an influential norm-setting statement by virtue of the political and economic power of its members.

In the 2016 Leaders' Declaration, G20 members signalled their commitment to data protection for the first time. In it, they commit to "respecting applicable legal frameworks for privacy, data protection" and "helping to ensure a secure ICT environment in which all sectors are able to enjoy its benefits" and reaffirm "the importance of collectively addressing issues of security in the use of ICTs".



### Should civil society engage?

For civil society in countries who are members of any of these mechanisms, the most important priority is to ensure the passage of comprehensive data protection at the national level.

In some cases, regional mechanisms require countries to pass a data protection law. For example, on the African continent, the AU and ECOWAS have both adopted instruments which require their members to implement a data protection law. Therefore, in countries with limited or no data protection legislation, membership of ECOWAS or the AU arguably gives civil society a stronger case in engaging with their governments to ensure that a comprehensive data protection law is implemented and enforced.

There have been suggestions that the UN should develop and pass a data protection treaty and that this is the only way to ensure an adequate level of data protection in each country at the national level. It is argued that, without a treaty, some countries are unable to participate in the development of data protection standards at the international level and will not, therefore, be incentivised to pass data protection legislation.

However, others argue that the existence of international binding legal instruments like Convention 108 and the EU's GDPR (discussed in detail on pp. 56-7) renders the need for a data protection treaty void, as these instruments set a strong international benchmark for data protection and will strengthen data protection norms and standards globally.

Regardless of whether a treaty is adopted by the UN on data protection, the most important avenue for ensuring data protection standards which protect human rights is through comprehensive regulation, which is implemented at the national level (see the first section of this chapter).



## The International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is a membership organisation of privacy and data protection authorities from around the world. At its annual Conference, members discuss and debate data protection issues. The outcomes of the annual Conference include resolutions and declarations which reference international standards and agreements and express general agreement and shared commitments among the members.

In 2005, members adopted the Montreux Declaration, which appealed to the UN to prepare a legally binding instrument clearly setting out data protection and privacy as enforceable human rights. And in 2009, the Conference adopted a “Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data”, which set out basic data protection principles and was meant to serve as an input to deliberations by the UN General Assembly on a data protection treaty.

For specific, tailored guidance on how to engage as a human rights defender in international forums like the G20, ICDPPC, and UNHRC, see our series Navigating the Digital Environment.

Find the series on [www.gp-digital.org](http://www.gp-digital.org).

## The Organization for Economic Cooperation and Development

The Organization for Economic Development (OECD) has had an important global influence on the setting of minimum data protection standards through the issue of its guidelines on the protection of privacy and transborder flows of personal data (see chapter 4), which is used around the world as a template



for the drafting of legislation and non-statutory standards relating to data protection. The OECD issued a lightly revised version of the guidelines in 2013, which – while leaving the ten minimum principles unchanged – placed greater emphasis on the accountability of data controllers, recommending that organisations implement privacy management programs at the organisational level, governments develop national privacy strategies, and that all data controllers ensure data subjects are provided with notices of security breaches which affect their personal data.

The OECD guidelines on Consumer Protection in E-commerce (1999) also include provisions related to privacy and data protection.

## Technical bodies

International bodies like the International Standards Organisation (ISO) play an important role in the development of norms around data and privacy-related issues, including biometrics, identity management, and cloud computing. Companies and public agencies may adopt standards to demonstrate compliance with national legislation and to make sure that their products are interoperable, and can therefore be sold and used by consumers in different countries.

Many countries also have national agencies which set standards or adopt standards developed by international bodies. In the US, for example, the National Institute of Standards and Technology (NIST) is responsible for developing standards which support federal agencies in meeting their obligations under the various data protection-related laws and regulations in the US.



### Should civil society engage?

Yes. Technical bodies develop standards which impact on data protection. For example, the use of encryption in the transmission and storage of data can assist data controllers in complying with data protection principles related to security. In this way, technical standards can support the effective implementation of legal frameworks. At the same time, technical standards are also important in ensuring the level of protection of individuals' personal data independently of what legal frameworks apply.

Where there are rarely formal opportunities for engagement at the organisational level in standards setting bodies, civil society can attend meetings and provide explanatory material to meeting participants which highlights the links between the development of technical standards and data protection. Some bodies have organs specifically dedicated to human rights considerations, such as the Human Rights Protocol Considerations Research Group at the Internet Engineering Task Force (IETF), and ICANN's Cross Community Working Party on its Corporate and Social Responsibility to Respect Human Rights.

Civil society can also reach out individually to the members of standards setting organisations. At the ISO, this would mean reaching out to the national representative organisation from the civil society group's respective country.

The leadership of technical bodies can have a strong influence over the position taken by a body on particular standards. Civil society should therefore monitor appointments to ensure they do not compromise the independence of the body – for example, if they are put forward by a particular country for strategic reasons.







## CHAPTER VI

# HOW CAN HUMAN RIGHTS DEFENDERS AND CIVIL SOCIETY ORGANISATIONS ENGAGE?





## How can human rights defenders and civil society organisations engage?

It's clear that the existence and enforcement of strong, consistent data protection laws is a key mechanism for protecting human rights. However, coverage varies globally.

Some countries still lack specific legislation, or have incomplete provision in other laws. And even in jurisdictions with stronger data protection, implementation or oversight may be weak.

Below, we set out some key messages, strategies and approaches for human rights defenders operating in different data protection regimes.

### COUNTRIES WITH WEAK OR SECTORAL DATA PROTECTION REGIMES

In countries where no data protection law exists, or where laws only partially address data protection, the first priority of civil society organisations should be to foster public awareness around data protection and lobby lawmakers to introduce or update legislation.

If a data protection law is under review or in process, push for it to be opened for public consultation. If you are able to contribute as a human rights defender, insist on the principles which should underpin a robust data protection law, as outlined in chapter 4 and annex 1 (pp. 89-92). The implementation of the EU's GDPR offers a useful reference point in terms of best practice.

Governments, of course, aren't the only stakeholder in data protection. Businesses have a responsibility, under the UN



Guiding Principles on Human Rights, to create products and services which protect the privacy of their users. In countries with a weak regulatory environment around data protection, however, businesses may lack the capacity and understanding to do this. Proactive engagement from civil society is vital. Here are a few key messages you might use to make your case:

- **Data protection is essential to the protection of human rights:**

In some countries, data protection is a right in and of itself.

But even where this is not the case, data protection is essential for the protection of human rights, in particular the right to privacy. The links between data protection and human rights are set out in more detail in chapter 3 of this guide.

- **Comprehensive data protection promotes access to markets and strengthens the digital economy:** Data protection is vital to consumer trust in products and services. Moreover, harmonising standards provides a competitive advantage to countries by opening up their markets to trade. This is particularly important for countries that seek to trade with the EU, as the EU has strict data protection requirements when it comes to providing services which involve the processing of personal data.

- **Data protection supports cybersecurity:** By imposing legal obligations on those who process data to implement security measures, data protection reduces the risk of data breaches or hacks of datasets. Data breaches include the alteration or theft of personal data for commercial, political or economic reasons. This can result in the loss or exposure of trade, intelligence and other state secrets, as well as serious reputational harm to businesses.



### Tools for engaging with tech businesses

Trying to work with businesses on data protection issues?

GPD has created a series of how-to-guides which may be useful: How to Respect Privacy and Free Expression as a Tech SME.

The guides offer practical resources, model scenarios, and a clear set of business-focused arguments for embedding responsible data practices in SMEs. They're currently available for Kenya, Senegal, Nigeria, South Africa and Mexico, but can be tailored for use in any country.

Find them on [www.gp-digital.org](http://www.gp-digital.org)

## COUNTRIES WITH A COMPREHENSIVE DATA PROTECTION REGIME

Even in countries where data protection laws are strong, human rights defenders have a responsibility to engage.

Take the EU, for example, which with the GDPR now has the strongest data protection regime in the world. In spite of this, states within the EU may still pass laws which enable data collection practices which can contravene human rights. In these cases, it's important to hold both businesses and governments to account for non-compliance.

It's also important to remember that many of the obligations and responsibilities contained in data protection laws like the GDPR will evolve in line with decisions and interpretations made by regulators and courts. In Hong Kong, for example, which was the first Asian country to adopt a comprehensive data protection law, the Office of the Privacy Commissioner for Personal Data takes a proactive role in publishing regulatory guidance.



## Data protection advocacy in the EU

In 2006, the EU passed its Data Retention Directive, which compelled internet service providers and other telecoms service providers in member states to store their users' data for between 6 and 24 months. A civil society group called Digital Rights Ireland initiated a legal fight against the Directive that same year, arguing that the mass data retention regime it required was disproportionate to the legitimate aims being pursued, and had insufficient safeguards in place, therefore violating the right to personal data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

The campaigners (mostly lawyers) built up a high media profile through engagement with journalists and regular blogs, which allowed them to establish themselves as expert voices. Through their membership of EDRI, a network of civil and human rights organisations from across Europe, they were also able to coordinate with other ongoing actions against the Directive, including a claim from Austria, which they merged into their own.

In 2014, the Court of Justice of the European Union (CJEU) invalidated the Directive for violating fundamental rights. Since then, other digital rights groups in Europe have used their approach as a template, with a civil society campaign against the UK's Data Retention and Investigatory Powers Act 2014 drawing on similar strategies. In 2016, the CJEU declared measures to compel general and indiscriminate data retention unlawful. Compliance in member states, however, remains uneven. The UK passed another controversial data retention law in 2016, the Investigatory Powers Act, which is currently subject to another legal challenge. In November 2017, the UK government admitted that "some aspects of the current regime (...) do not satisfy the requirements of the CJEU's judgment".



In recent years, it has issued guidelines and code of practice on issues such as data breach notifications, data protection in the workplace, and subject access requests.

At the time of writing, Argentina's Data Protection Law is being revised in order to bring it in line with the GDPR so that it can continue to trade with the EU. The proposed changes include the inclusion of biometric and genetic data as personal data, as well as measures to strengthen the independence of the National Directorate for Personal Data Protection, the supervising authority in charge of compliance with data protection. In South Korea, where the law has also been amended in response to mass data breaches, data controllers are subject to strict regulation, including the requirement to undertake "technical, managerial and physical measures" to protect data from breaches and to notify data subjects in case of a breach. The law also requires controllers to provide notice to data subjects about the processing of their data in a way that is "concise, transparent, intelligible and easily accessible; written in clear and plain language", with data controllers subject to heavy fines for non-compliance.

Even in countries with comprehensive data protection legislation, civil society has an important role to play as a watchdog, following the evolutions of data protection law and its applications, and ensuring that the rights of the data subject are being respected.





## Glossary

**Artificial intelligence:** Sometimes used interchangeably with “machine-learning”, artificial intelligence refers to the ability of computers to exhibit behaviour or thought that is normally demonstrated by humans or requires intelligence in order to solve complex problems.

**Algorithm:** A formula or a list of rules which is followed in order to answer a predetermined question or problem. Often deployed using large data-sets.

**Big data:** The use of advanced analytic techniques on large, complex datasets.

**Cloud:** a network of data centres connected over the internet. “Cloud computing” is the delivery of on-demand computing resources over the internet.

**Data controller:** a person who (either alone or with others) determines the purposes for which personal data is processed, and in what manner.

**Data processor:** a person who (either alone or with others) processes personal data on behalf of the data controller.

**Data processing:** the range of actions on data which processing can refer to includes: 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.



**Data protection:** also known as data privacy, data protection refers to the regulation of data processing.

**Data protection authority:** public authorities that supervise the application of the data protection regulation.

**Data subject:** any individual person who can be identified directly or indirectly by a piece of information, and who has rights under data protection regulation.

**Internet of things:** the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

**Open data:** data that can be freely used, re-used and redistributed by anyone.

**Personal data:** any data which relates to an identified or identifiable individual.

**Profiling:** the automated processing of personal data to evaluate certain aspects of that person, often in order to analyse or predict aspects of them, such as their performance at work, economic situation, health, personal preferences, interests, behaviour, location, or movements.

**Terms of service:** the set of rules and regulations that apply to the use of a software or internet-based product or service.



# Appendix

## ANNEX I

### The ten minimum standards

**1. Fairness and lawfulness:** Personal data should be collected (and thereafter stored and used) fairly and lawfully. This means that, wherever possible, data should only be collected (and stored and used) with the knowledge and consent of the data subject, and always in accordance with the law. It should not be permissible, for example, to trick someone into providing personal data, or to obtain it unlawfully by stealing it or hacking into their devices. Convention 108 contains a further requirement, not found in the OECD Privacy Guidelines, namely that certain special categories of personal data which reveal a person's racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, or data relating to criminal convictions, should not be processed automatically at all unless the law provides for appropriate safeguards.

**2. Data quality:** Personal data should be adequate, relevant and not excessive in relation to the purposes for which it is stored and used. This means that it should be accurate, complete and, where necessary, kept up to date. To give an example, an employer would have a legitimate interest in knowing certain information relating to any disabilities and the health status of its staff for purposes of accommodating any disabilities or for health and safety reasons. But certain health information – such as blood type or genetic disorders – meets neither of these purposes and it would be excessive for the employer to require and store it. If the disability or health status of a staff member changed, then the employer should ensure that this is reflected in the information they store. Further, personal data should not be kept for any longer than is required for the purpose or purposes for which it is



stored. To continue using the above example, information about a staff member's disabilities or health status is only necessary while they are employed at that company. If a staff member leaves the company, the information should be deleted from the employer's records.

**3. Purpose specification:** Personal data should be collected, stored and used for legitimate purposes only and not in a way which is incompatible with those purposes. The purposes for which the personal data is being collected should be specified at or before the time of the data's collection. So, while a hospital would have a legitimate interest in collecting the contact details of patients to communicate with them on issues related to their treatment at that hospital, it would not be a legitimate purpose for a staff member to use those details to contact patients to inform them of a friend's physiotherapy clinic to boost business.

**4. Notice of purpose:** The data subject should be informed of the purposes for which their data is being collected, stored and used at or before the time of its collection. They should also be informed of the rights that they have in relation to that data, including to withdraw consent for its use, to receive a copy of the data at any time, and to have it corrected or deleted.

**5. Limited use:** Personal data should not be used or disseminated for purposes other than those specified at the time of its collection except with the consent of the data subject or by the authority of law. If, for example, a university holds the home addresses of its students solely for the purpose of contacting them on study-related matters, it should not be permissible for the university to pass these details on to others, such as recruitment agencies, without the students' consent. However, if separate legislation empowers, for example, the police to demand information about individuals who have gone missing, and the police ask for the home address of a student who has disappeared, the university would not be in breach of this principle in providing that information.



**6. Security:** As a result of the risks to an individual's privacy that might arise if their personal data is lost, stolen or leaked, data protection legislation should require data controllers to take appropriate security measures. These measures should include those reasonably required to secure the protection of personal data against accidental or unauthorised destruction, accidental loss, and unauthorised access, alteration or dissemination. What those measures will look like in practice will depend on the size of the organisation; the type of information and data which is collected, processed and stored; the form of such information and data (e.g. on computer servers, the cloud, or physical files). They should include staff training on data protection, technical security measures such as the use of passwords and encryption, limiting access to certain staff members, and organisational measures which provide for the confidentiality, integrity, availability and resilience of processing systems.

**7. Openness:** Given that personal data relating to individuals may be collected without their knowledge, data protection legislation should require a body – whether a public authority, a private business or otherwise – to inform individuals when it collects personal data about them. There should also be means readily available for an individual to discover the existence and nature of personal data which has been collected, the purposes of its storage and use, as well as the identity and usual residence of the data controller.

**8. Access:** Individuals should also be able to request, without excessive delay or expense, any personal data which has been collected, in an intelligible form. If a data controller refuses such a request, reasons should be given, and the individual should be able to challenge the refusal.

**9. Correction or deletion:** An individual should be able to have corrected or deleted any data which is inaccurate or which was processed contrary to the above principles.



**10. Accountability, sanctions and remedies:** Data controllers should be accountable for complying with the requirements of the data protection legislation. It is a well-established principle of international human rights law that there should be appropriate remedies available and sanctions in place where an individual's human rights have been breached. Data protection legislation should therefore provide individuals with a remedy if any request to obtain or correct personal data is not complied with. The legislation should also set out the sanctions that may be imposed where a data controller or processor breaches the law, such as financial penalties or requirements to take steps to remedy the breach.

## ANNEX 2

### Exceptions to the right to privacy

The right to privacy is not an absolute right, and there are certain circumstances where what would otherwise be a breach of the right to privacy can be justified and permissible. There is a three part test for justification; if there are to be any permitted exceptions to the general rules and principles set out above, these will constitute a breach of the right to privacy unless they comply with this three-part test. This is explicitly recognised by Convention 108 (although not the OECD Privacy Guidelines) which permits states parties to derogate from provisions in the Convention in circumstances where the three-part test is met.

#### 1) Any restrictions or interferences must be 'provided for by law'

The first part of the test is that any restrictions or exceptions must be 'provided for by law'. In practice, this means that they should be set out clearly within legislation. In order to ensure clarity, best practice dictates that these any restrictions or exceptions should be set out in the data protection legislation



itself, rather than in other pieces of legislation which might deal with, for example, surveillance, or the powers of security or law enforcement agencies.

### 2) They must be in pursuance of a 'legitimate aim'

The second part of the test is that any restrictions must be in pursuance of a 'legitimate aim'. While the precise wording of 'legitimate aims' varies among different international human rights instruments, they can be summarised as:

- Protecting the rights and freedoms of others;
- Protecting national security;
- Preventing crime;
- Protecting public safety and public order;
- Protecting the state's economic and monetary interests.

### 3) They must be 'necessary' to meet that aim

The third part of the test is that any restrictions, as well as being in pursuance of a legitimate aim, should be 'necessary'. This also includes an assessment of proportionality. While there is no single universal definition of 'necessary' and 'proportionate', the European Court of Human Rights has interpreted the former to mean something more than 'useful', 'reasonable' or 'desirable'. (See, for example, *Handyside v. United Kingdom*, Application No. 5493/72, (1976))



## Best practice on exceptions

The EU's General Data Protection Regulation applies directly to all EU member states and came into force in May 2018. The Regulation sets out various requirements of data controllers and data processors as well as a number of rights of data subjects. Article 23 makes clear that EU member states can only take legislative measures which restrict the rights of data subjects set out in the Regulations if they "[respect] the essence of the fundamental rights and freedoms and [are] a necessary and proportionate measure in a democratic society to safeguard" one of ten specified legitimate aims:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- (e) other important objectives of general public interest of the EU or a member states, in particular important economic or financial interests, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to above;
- (i) the protection of the data subject or the rights and freedoms of others; and
- (j) the enforcement of civil law claims.



## ACKNOWLEDGEMENTS

This guide was researched and authored by the Global Partners Digital team. Special thanks go to Carly Nyst and Dr. Evelyne Sørensen for their review and feedback.

Produced by The Kitchen agency

Designed by Miriam Hempel | Illustrations by Valentina Cavallini





In the digital age, the processing of personal data offers undeniable opportunities for economic growth, social advancement and research.

It can also, without adequate safeguards, pose risks to the rights of individuals – particularly their right to privacy.

The processing of personal data is regulated by a set of frameworks known as data protection, and over 100 countries around the world have data protection legislation. However, the extent of coverage varies greatly. At the same time, the fragile balance which the original data protection principles sought to preserve – allowing free flow of data while also preserving user rights – is being tested by technological developments which have radically increased the scale and depth of personal data processing.

That's where this guide comes in. Designed specifically for human rights defenders, it offers a comprehensive and accessible introduction to the world of data protection - explaining the history of personal data processing, the key debates, why they relate to human rights, and where - and how - you can engage.

Data Protection for Human Rights Defenders is the fifth entry in the Travel Guide to the Digital World series. Find the rest of the series on [www.gp-digital.org](http://www.gp-digital.org).

