PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

General Provisions, Definitions and Scope

General Provisions, Definitions and Scope

General Provisions

Object and purpose of the law

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

The following should be included:

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

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

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

Object of Convention 108 modernised to protect individuals

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

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

Definitions

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

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

Personal data

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

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

An example definition from the EU GDPR is:

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

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

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

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

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

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

Examples of personal data

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

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

Sensitive personal data

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

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

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

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

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

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

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

Processing

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

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

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

An example definition is:

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

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

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

Data controllers and data processors

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

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

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

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

Profiling

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

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

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

Scope and Application of the Law

Material scope

What should the regulation apply to?

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

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

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

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

Public and private institutions: two entities, two regulations

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

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

Who should the regulation apply to?

It is essential that this section of any law provides clarity as to whom the law applies. Data protection legislation should apply to both public and private institutions. It is unacceptable practice that public institutions (including law enforcement and intelligence agencies) be completely exempt from having

obligations to protect the personal data of data subjects, or for exemptions to be excessively wide or vague.

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

Examining Exemptions

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

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

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

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

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

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

The law should specifically provide for the development and inclusion of standards applicable to the protection of personal data which is collected and processed for the purposes of public safety, defence, state security and investigation or prevention of criminal offences.

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

Exceptions

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

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

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

Human right mechanisms and CSOs express concern about intelligence-sharing

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

brought into line with the regime of international transfers of personal data contained elsewhere in the law.

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

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

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

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

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

Territorial scope of application

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

they are based.

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

- Applies to controllers and processors established in the country, even if the processing takes place outside the jurisdiction of the country[8]
- Applies to the processing of personal data by controllers and processors established outside the jurisdiction of the country where the individual is based
- Regulates the conditions for transferring of personal data outside the territory of the country.

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

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

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

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

References

1 Article 5 of the Law 1581 of 2012 of Colombia

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

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

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

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

6 This is the definition provided for within GDPR.

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

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

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

PRIVACY INTERNATIONAL

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

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

UK Registered Charity No. 1147471