PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 3:

Data Protection Principles

Fair, lawful and transparent

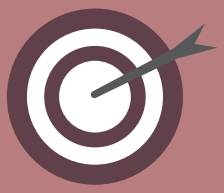
The processing of personal data should be lawful and fair and done in a transparent manner.

Purpose limitation

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

Minimisation

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



Accuracy

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

Storage Limitation

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

Integrity and Confidentiality

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

Accountability

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

Data Protection Principles

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

Fair, Lawful, and Transparent

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

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

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

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

Why does this principle matter?

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

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

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

Purpose Limitation

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

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

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

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

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

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

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

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

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

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

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

These could include, but are not restricted to:

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

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

Why does the purpose limitation principle matter?

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

Minimisation

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

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

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

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

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

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

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

Why does the data minimisation principle matter?

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

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

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

Accuracy

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

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

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

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

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

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

Why does the accuracy principle matter?

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

Storage Limitation

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

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

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

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

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

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

Why does the storage limitation principle matter?

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

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

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

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

Integrity and Confidentiality

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

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

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

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

Security safeguards could include:

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

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

Why does the security safeguards principle matter?

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

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

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

Accountability

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

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

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

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

Why does the accountability principle matter?

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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