PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 6:

Obligations of Data Controllers and Processors

Compliance and Accountability

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

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

Recording Processing Activities

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

Q: Does the law:

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

Such as

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

Safeguarding Security, Integrity and Confidentiality

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

Q: Does the law:

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

Suggested obligations could include but are not limited:

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

Adopting data protection by design and by default

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

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

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

Impact assessments

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

Q: Does the law:

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

An impact assessment requires at minimum assessment of:

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

Data Protection Officers

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

Q: Does the law:

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

Notification of breach

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

Q: Does the law:

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

Notification should include at minimum details about:

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

Obligations of Data Controllers and Processors

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

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

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

Compliance with the Law

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

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

This may include:

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

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

Recording Processing Activities

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

The information could include:

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

Integrity and Confidentiality

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

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

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

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

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

Pseudonymisation: Not a Silver Bullet for Complying with Data Protection

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

Examples of provisions on pseudonymisation:

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

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

Under the GDPR:

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

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

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

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

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

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

Privacy by Design and by Default

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

Privacy by design

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

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

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

Privacy by default

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

Impact Assessments

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

An impact assessment requires, as a minimum:

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

Data Protection Officers

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

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

Notification of Breach

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

This obligation should be clearly stipulated in law and provide:

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

Definitions of 'data breach':

GDPR: "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed [Article 4 (12)]."

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

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

Example of Guidance for Responding to Breaches

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

International Data Transfers

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

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

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

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

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

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

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

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

Examples of Adequacy Mechanisms

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

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

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

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

Exceptions

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

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

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

References

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

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

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

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

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

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

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