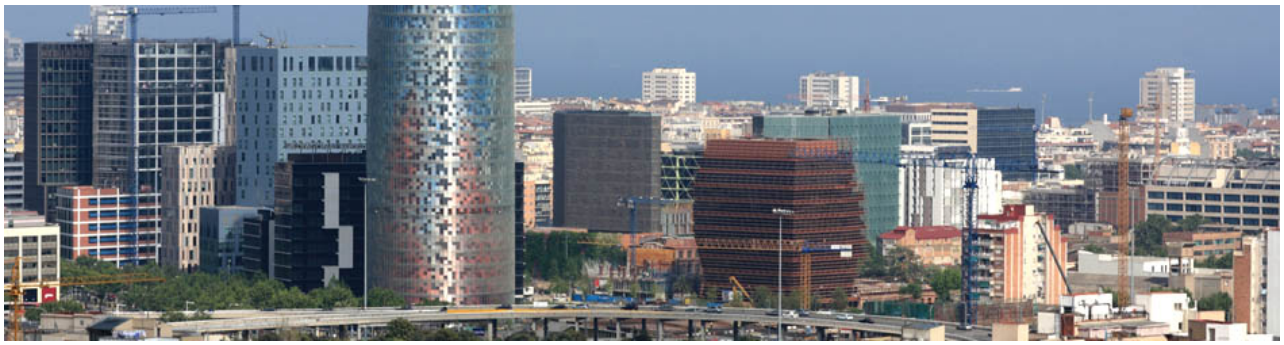
DATA PROTECTION LAWS OF THE WORLD

Spain

DLA PIPER

SPAIN



Last modified 22 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

After a long delay the Spanish Parliament approved the new Spanish Fundamental Law on Data Protection and digital rights guarantee developing and refining the GDPR in December 2018. It has been in force from 7 December 2018 **(“NLOPD”).**

DEFINITIONS

"Personal data" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4 of the GDPR). A low bar is set for "identifiable" – if the natural person can be identified using *“all means reasonably likely to be used”* (Recital 26 of the GDPR) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

NLOPD is extremely restrictive regarding the processing of criminal convictions and offences data, that shall be forbidden except in very exceptional circumstances. Spain deviates itself notably in this regard from the standard position in the EU, where this prohibition is not usually so strict.

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Despite following GDPR’s approach in this regard, NLOPD does also regulate certain features related to personal data of deceased people.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities. The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **"lead supervisory authority"**. Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Spanish competent national supervisory authority is the *Agencia Española de Protección de Datos* (“**AEPD**”), which also represents Spain on the European Data Protection Board. Regional Data Protection Commissioners do exist to supervise personal data processing by regional public authorities and other entities controlled by regional public authorities.

Contact details of the AEPD

Address

C/Jorge Juan, 6
28001 Madrid
Spain

Telephone

+34 901 100 099 /
+34 91 266 35 17

Website

www.aepd.es

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities. The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

NLOPD requires to do so, even for voluntarily appointed DPOs within a short period of time (10 days).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely.

The NLOPD includes a lengthy list of organisations and companies that are required to appoint a DPO. Accordingly, insurance or reinsurance companies, financial credit institutions, educational institutions, electric and natural gas distributors, and advertising and marketing companies, among others, are required to appoint a DPO. The NLOPD also allows organisations and companies to voluntarily appoint a DPO. Please note that, in either case, the appointment of the DPO must also be communicated to the AEPD using the AEPD online facilities.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or

- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Indeed, NLOPD has done so in a very intense manner. In 2023, the Spanish AEPD confirmed a new and stricter approach regarding the use of biometric data for monitoring access to offices / workplaces, that should be allowed for the future only in very exceptional circumstances.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

The NLOPD has confirmed this prohibition in very strict terms, with only very extraordinary exceptions (e.g. activities of lawyers and court representatives acting on behalf of their clients, verification imposed by AML law, verification imposed by child-protection law).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors

that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xls / .xlsx).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Data protection principles

The NLOPD foresees certain scenarios where the controller shall not be responsible for inaccurate data (provided it has taken all reasonable measures to ensure deletion or rectification without delay).

Criminal Convictions and Offences data

Article 10 of the NLOPD allows lawyers and procedural representatives to process the information provided by their clients related to criminal convictions and offences for the purposes of rendering the corresponding legal services. There are also other isolated exceptions if and when endorsed by the law (e.g. verification imposed by AML law, verification imposed by child protection law).

Processing of administrative offence or penalties

The processing of personal data related to administrative offences or penalties is permitted if it is carried out by the relevant public bodies having sanctioning powers over such offenses, and only to the extent necessary for achieving their legitimate purposes. If those requirements are not met, the processing shall be allowed by an specific law, or be based on the data subject’s consent.

Please note that lawyers and procedural representatives are also allowed to process the information provided by their clients related to administrative offenses or penalties for the purposes of rendering the corresponding legal services.

Credit Solvency Databases

The NLOPD sets out stringent requirements for including personal data on credit solvency databases. In this regard, the information to be provided to data subjects as well as the particularities of the debt are, among others, key aspects to be taken into account.

CCTV Processing

Under the NLOPD, the processing of images through CCTV is only permitted for security purposes, provided that (i) the data obtained is duly deleted within the corresponding period of time (unless it is relevant for evidence purposes), and (ii) the mandatory notice requirements are met. Additional detailed requirements do apply.

Whistleblowing

The processing of personal data relating to whistleblowing (including anonymous reporting) is permitted provided that (i) employees are duly informed ,(ii) whistleblowing databases are only accessed by the necessary persons to carry out internal control purposes or to initiate the relevant disciplinary proceedings, and (iii) the data obtained is duly deleted within the mandatory period of time. Additional detailed requirements do apply.

Unfair competition

The NLOPD generates a new catalogue of “unfair competition practices” linked to personal data.

Data processing for electoral purposes

Political parties, coalitions and electoral groups can use personal data obtained from websites and other public sources to carry out political activities during an election period. Likewise, sending electoral propaganda by electronic means, as well as contracting any such propaganda on social or similar networks will not be deemed a commercial activity.

Transparency (Privacy Notices)

The NLOPD allows (Article11) provision of the information required by Articles 13 and 14 of the GDPR in layers. In this sense, a first layer should include the “basic information” of the relevant processing as well as an immediate and easily accessible form (i.e. a link) to the second layer, where the rest of information to be provided under Articles 13 and 14 of the GDPR shall be included. Please note that the content of the before-mentioned “basic information” depends on each case, but most of the times includes (i) the identity of the controller, (ii) the purpose of the processing, and (iii) the rights under Article 15 – 22 of the GDPR.

Rights of the data subject

Under the NLOPD, a data subject’s right of access is deemed granted when the controller provides him/her with a means that permanently guarantees remote, direct and secure access to his / her personal data. In addition, the NLOPD indicates that more than one right of access request within six months shall be considered repetitive for the purposes of Article 12(5) of the GDPR unless the relevant requests are based on a legitimate reason.

Under the NLOPD, controllers must clearly indicate in their internal information systems the cases where the processing of personal data is restricted.

Blocking right / Blocking duty (NLOPD)

The NLOPD states that following the exercise of rectification or erasure, controllers shall "block" the personal data so that it shall remain available to the relevant public authorities in very specific situations. The NLOPD also offers other alternatives in case the “blocking” of personal data is not feasible or involves a disproportionate effort.

Rights of the deceased

The NLOPD recognizes the right to digital testament. Moreover, the heirs of the deceased are entitled to exercise the rights of access, erasure and rectification of data unless the deceased person would had prohibited it (or if it is not in line with applicable law).

Special category data

The NLOPD deviates from GDPR mainstream approach on special category data. Most of this type of data cannot be processed relying on the consent of the data subject (health, biometric and genetic data being the exception to this ban, but relying on consent may be also not permitted for the latter and even standard data in employment and other contexts).

Location data

The overall position in Spain is that it may be acceptable provided that:

- users are informed at all times on whether the location system is active and retain full control on the system, freely deciding when to switch it on or off;
- the purposes of the processing are legitimate and proportionate and do not harm in an unfair manner the constitutional rights of the data subjects;
- users have been clearly informed on the circumstances under which they can be located and the purposes of such processing;
- users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system; and
- if in an employment context, Works Council / representatives of the employees, have been informed in advance about the collection of this type of information and the purposes of the processing (which shall remain within the limits of the authority of the employer to direct, control and monitor workers’ professional activities)

One of the main originalities of the NLOPD when compared with the GDPR is that it accepts new “digital rights”, including, i.e. Internet neutrality, universal access to Internet, security of online communications, digital education, protection of minors on the Internet, amendment / update of non-accurate information on the Internet, a right to be forgotten-like right not to be found by search engines on the Internet and social networks.

On top of this, certain provisions of the NLOPD may have an impact on the relationship between a company and its employees (i.e. monitoring of digital devices, digital disconnection of the employees outside working hours, privacy at the workplace).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). As of 29th November 2022, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, the Eastern Republic of Uruguay, New Zealand, the Republic of Korea (South Korea) and the United Kingdom.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules or EU/AEPD standard contractual clauses (a new version of which was approved by the EU Commission in June 2021). The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities (which remains under NLOPD, however, when EU/AEPD standard contractual clauses are replaced by other sets of clauses or other safeguards).

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*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). No minimum threshold, in terms of individuals concerned or financial impact of the breach is set by GDPR or NLOPD regarding the notification obligations.

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

NLOPD has established different levels of infringements (very serious, serious and minor) which are linked to different limitations’ periods (3, 2 and 1 year respectively).

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, since the AEPD defends the viewpoint that e-Marketing laws are more specific than GDPR/NLOPD and shall prevail on the latter when data protection and e-marketing elements do concur (a problem that would not be present when marketing deliverables are provided off electronic channels, in which case other legal bases for processing, like the legitimate interest of the sponsor could be considered again). Where consent is relied upon, AEPD claims that the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is expected to be replaced very soon by a EU-level Regulation, whose drafting procedures are nearly finalised. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive shall be replaced, the AEPD claims, with the GDPR standard for consent.

Electronic Marketing is regulated in Spain specifically by the Spanish Act on the Information Society Services and e-Commerce 34 /2002 ('LSSI'). The general principle is that deliveries of electronic marketing materials are lawful only if they have been explicitly authorised in advance by the recipients (authorisation that is required not just for individuals, but also where the recipient is a legal entity, broadening here the scope of Spanish Data Protection Act). An exception to this general principle applies to deliveries to clients when the materials refer to products/services that are equal or similar to the ones sold to them in the past by the company sponsoring the advertisement.

Electronic publicity shall:

a. be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line,
b. allow the recipient to opt-out at all times, even at the time of registration, and
c. clearly identify the sponsor of the delivery. It is the sponsor of the delivery, not the electronic publicity company that shall be held liable in case of enforcement. Opt-out shall include an email address when the publicity was delivered by email too. Opt-out procedure shall be simple and free for the recipient of the publicity.

Enforcement shall include, *inter alia*, fines that, in most cases, shall be between EUR 30,000 and EUR 150,000.

The NLOPD states that databases containing the identification details of those data subjects who have expressed their opposition to receiving commercial communications may be created (the so-called “**Robinson’s Lists**”). These databases must be reviewed by the entities sending commercial communications (the access details to these databases will be published by the AEPD) unless the relevant data subjects have previously granted their consent to receiving such commercial communications.

Finally, it shall also be taken into account that that the NLOPD permits processing activities where the purpose is to avoid sending commercial communications to those data subjects who have expressed their opposition to receiving them.

ONLINE PRIVACY

Cookies are regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce (“**LSSI**”), as amended in March 2012. In July 2023, the AEPD released new Guidance Notes on the use of cookies (granting a sunrise period until 11th January 2024 for the data controllers and data processors to implement the new criteria). Although the Guidance Notes are not legally binding they give useful indications on the best market practice and on the criteria that the AEPD would follow when enforcing the law.

The Guidance Notes require data controllers to inform cookies’ recipients – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. The regulator stresses the need for cookies’ sponsors to make sure (and be able to demonstrate later on) that the user has noticed the invitation to install and use the cookies and has voluntarily and unmistakably decided to accept it. Certain types of cookies (e.g. session cookies) are exempt from these restrictions.

KEY CONTACTS

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

Paula González de Castejón
Partner
T +34 91 788 7374
paula.gonzalez@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.