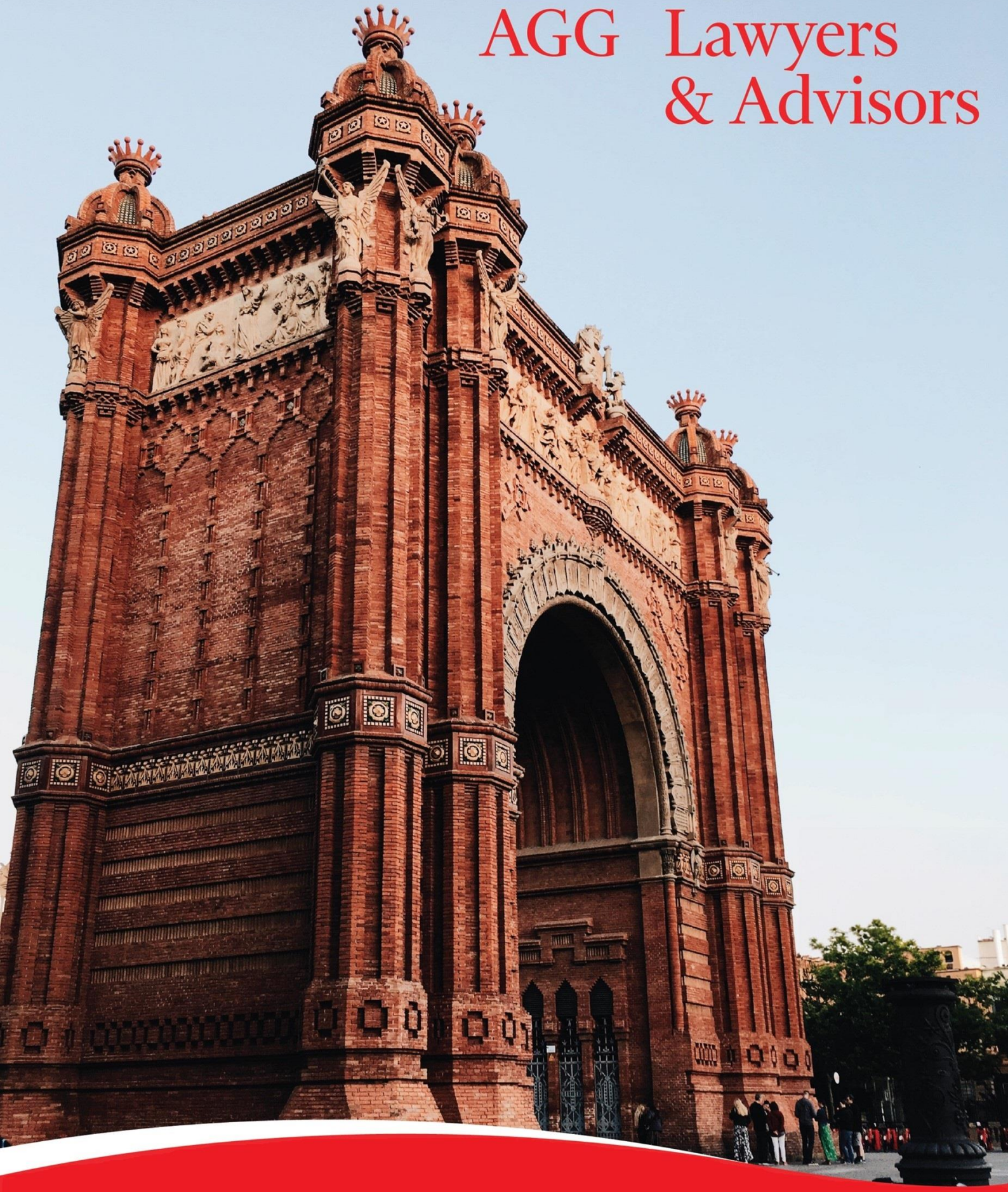
AGG Lawyers & Advisors



Data Protection & Privacy Laws in Spain

1. Introduction

The GDPR (EU) 2016/679, effective since May 25, 2018 (**GDPR**), alongside the Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (**LOPDGDD**), serves as the cornerstone of personal data protection in Spain.

The GDPR is a comprehensive regulation that applies to any organization, regardless of its location, that processes the personal data of EU residents. This regulation sets stringent guidelines and principles to ensure the protection of personal data and uphold the privacy rights of individuals.

The LOPDGDD complements and adapts the GDPR's principles to the Spanish legal framework, introducing specific requirements tailored to the national context. It encompasses additional measures such as dedicated provisions for digital rights, addressing issues like internet privacy, digital education, and the security of electronic communications.

Together, these laws create a robust legal landscape aimed at enhancing data protection, increasing transparency, and ensuring that individuals maintain control over their personal information.

Compliance with these regulations is not only a legal obligation but also a crucial aspect of building trust and integrity in business operations.

2. Key Definitions

A. Personal Data

As defined by Article 4 of the GDPR, personal data includes any information relating to an identified or identifiable natural person. This can include names, identification numbers, location data, and online identifiers.

Examples: Name, ID number, photo, email address, IP address.

B. Processing

Processing refers to any operation performed on personal data, whether automated or not, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, and destruction.

C. Data Subject, Data Controller, and Data Processor

i. Data Subject

The individual whose personal data is being processed.

ii. Data Controller

The entity determining the purposes and means of processing personal data.

iii. Data Processor

The entity processing personal data on behalf of the controller.

D. Special Category Protection

Includes data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning a natural person's sex life or sexual orientation.

3. Data Protection Rights and Responsibilities

A. Rights of Data Subjects:

i. Right to be Informed

Transparency about how personal data is collected and used. When the data controller obtains personal data from a data subject, they must inform them using clear and simple language about the contact details of the controller, purposes of processing, retention period, data subject rights, and the right to lodge a complaint with the supervisory authority.

ii. Right of Access

Data subjects can request access to their personal data and obtain information on how it is processed.

iii. Right to Rectification

Correction of inaccurate or incomplete data.

iv. Right to Erasure

The right to have personal data deleted under certain conditions, such as when the data is no longer needed for its original purpose.

v. Right to Restrict Processing:

Limit the processing of personal data under specific circumstances.

vi. Right to Data Portability

Transfer of personal data to another service provider.

vii. Right to Object

Objection to the processing of personal data in certain cases.

viii. Rights Related to Automated Decision-Making

Safeguards against decisions made without human intervention, including the right to not be subject to decisions based solely on automated processing, such as profiling.

B. Responsibilities of Data Controllers and Processors:

i. Lawful Processing

Personal data must be processed lawfully, fairly, and transparently. This includes obtaining explicit consent from the data subject or processing data based on other legal bases such as contractual necessity, legal obligations, legitimate interests, vital interests, or public tasks.

ii. Purpose Limitation

Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

iii. Data Minimization

Processing only the data necessary for the purposes stated.

iv. Accuracy

Keeping personal data accurate and up-to-date. Inaccurate data should be corrected or deleted promptly.

v. Storage Limitation

Retaining data only as long as necessary for the stated purpose.

vi. Integrity and Confidentiality

Ensuring appropriate security of personal data to protect against unauthorized or unlawful processing and accidental loss, destruction, or damage.

4. Legal Basis for Data Processing

A. Consent

Must be freely given, specific, informed, and unambiguous. Consent must be explicit for processing special categories of personal data.

Data subjects must be able to withdraw consent easily at any time.

B. Contractual Necessity

Processing is lawful if necessary for the performance of a contract with the data subject, such as processing data required to formalize a contract.

C. Legal Obligation

Processing is lawful if necessary for compliance with a legal obligation to which the data controller is subject.

D. Legitimate Interests

Processing is lawful if necessary for the legitimate interests of the data controller, provided these interests are not overridden by the data subject's rights and freedoms.

5. Data Protection Officer (DPO)

A. Role and Responsibilities

i. Monitoring compliance with GDPR and LOPDGDD.
ii. Advising on data protection obligations.
iii. Acting as a contact point for data subjects and supervisory authorities.
iv. The DPO must be involved properly and in a timely manner in all issues relating to the protection of personal data.

B. Qualifications and Appointment

i. Expertise in data protection law and practices.
ii. Appointed based on the scale and sensitivity of data processing activities.

iii. Organizations must ensure that the DPO is provided with sufficient resources to fulfill their duties and maintain their expert knowledge.

6. Data Breaches

A. Definition and Examples:

A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. Examples include hacking incidents, data theft, or loss of data due to system failures.

B. Notification Requirements

i. Notify the Agencia Española de Protección de Datos (**AEPD**) within 72 hours of becoming aware of the breach.
ii. Notify affected data subjects without undue delay if the breach poses a high risk to their rights and freedoms.

C. Procedures and Timelines

i. Immediate investigation and mitigation of the breach.
ii. Detailed documentation of the breach and response actions, including the nature of the breach, categories and approximate number of data subjects and personal data records concerned, and measures taken or proposed to address the breach.

7. Data Processing Agreements

A. Content Requirements

i. Processing purposes, duration, and nature.
ii. Types of personal data and categories of data subjects.
iii. Obligations and rights of the data controller and processor, including ensuring that processors only act on the controller's documented instructions.

B. Responsibilities of Data Processors

i. Processing data only on documented instructions from the controller.
ii. Implementing appropriate security measures to protect personal data.
iii. Assisting the controller in ensuring compliance with GDPR obligations, such as data subject rights and breach notifications.

8. Data Transfers Outside the EU

When a company in the EU needs to transfer personal data to a country outside the EU, there are specific rules to ensure that the data remains protected. These rules are in place to make sure that the data receives the same level of protection as it would within the EU.

A. Adequacy Decisions

The European Commission can decide that a third country, a territory, or a specific sector within that country ensures an adequate level of data protection. This means that the country's data protection laws are essentially equivalent to those of the EU.

If a country is recognized as having adequate protection, personal data can be transferred to it without any additional safeguards. Examples include countries like Switzerland, Canada (for commercial organizations), and Japan.

B. Appropriate Safeguards

If a country does not have an adequacy decision, companies can still transfer data by using specific tools and agreements that ensure data protection:

i. Standard Contractual Clauses (SCCs)

These are legal contracts approved by the European Commission that both the sending and receiving parties must agree to. They include specific data protection commitments.

ii. Binding Corporate Rules (BCRs)

These are internal rules for multinational companies, approved by EU data protection authorities, which allow transfers within the same corporate group to ensure data protection.

iii. Codes of Conduct

Industry-specific codes of conduct approved by a supervisory authority can provide a framework for ensuring data protection.

iv. Certification Mechanisms

Certifications, such as those issued by data protection authorities, indicate that the organization meets certain data protection standards. Organizations that receive such certifications can more easily transfer data internationally.

C. Derogations:

In certain cases, data can be transferred to countries without adequate protection or specific safeguards. These exceptions, or derogations, include:

i. Explicit Consent

If the individual (data subject) gives clear, informed consent to the transfer, understanding the risks involved due to the absence of adequate protection.

ii. Performance of a Contract

When the transfer is necessary to fulfill a contract with the individual, such as processing transactions for international travel bookings.

iii. Public Interest

When the transfer is needed for reasons of public interest, such as international data exchanges between tax authorities or for public health emergencies.

iv. Legal Claims

When the transfer is necessary for the establishment, exercise, or defense of legal claims.

v. Vital Interests

When it's necessary to protect the vital interests of the data subject or other people, especially in life-and-death situations.

9. Rights and Remedies for Data Subjects

Data subjects, or individuals whose personal data is being processed, have specific rights and remedies under the GDPR and LOPDGDD to ensure their data is protected and they can address any issues related to their personal data.

A. Lodging Complaints

If an individual believes their personal data has been mishandled or their data protection rights have been violated, they have the right to file a complaint with a supervisory authority.

Once a complaint is lodged, the AEPD will investigate the matter. This might involve examining the practices of the data controller or processor, requesting information, and evaluating whether the GDPR or LOPDGDD has been violated.

The AEPD can issue decisions requiring the data controller or processor to take specific actions to comply with data protection laws, impose fines, or provide other remedies to the data subject.

B. Judicial Remedies

Data subjects have the right to seek judicial remedies if their data protection rights have been infringed. This means they can take legal action against data controllers or processors.

i. Claiming Compensation

If an individual has suffered material or non-material damage due to a violation of their data protection rights, they can claim compensation from the data controller or processor responsible for the breach.

ii. Legal Proceedings

Legal proceedings can be initiated in the courts of the EU member state where the data subject resides, where the data controller or processor is established, or where the alleged infringement occurred.

iii. Court Orders

Courts can issue orders to stop data processing activities, rectify data handling practices, or provide other appropriate relief to the data subject.

10. Compliance and Best Practices

A. Data Protection Impact Assessments (DPIA)

A DPIA is a process designed to help organizations identify and minimize the data protection risks of a project. DPIAs are particularly important when introducing new technologies or processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

A DPIA is required whenever a data processing activity is likely to result in a high risk to data subjects. This could include large-scale processing of sensitive data (such as health information); systematic monitoring of publicly accessible areas (such as CCTV systems); and, processing that involves profiling or other forms of automated decision-making with legal or similarly significant effects.

B. Data Protection by Design and by Default

Integrating data protection into processing activities from the outset. Ensuring that only necessary data is processed, and data protection principles are applied at every stage of data processing.

C. Training and Awareness

Regular training for employees on data protection principles and practices. This includes understanding their responsibilities, recognizing potential data breaches, and responding appropriately.

D. Regular Audits and Reviews

Conducting regular audits to ensure ongoing compliance with data protection laws. Reviewing and updating data protection policies and procedures to address any new risks or regulatory changes.

11. Penalties and Enforcement

The GDPR and the LOPDGDD establish strict penalties and enforcement mechanisms to ensure compliance with data protection laws. These penalties can be significant, underscoring the importance of adhering to these regulations.

A. Types of Penalties and Fines

i. Administrative Fines

The LOPDGDD, in alignment with the GDPR, specifies two tiers of administrative fines for non-compliance. These fines are intended to be effective, proportionate, and dissuasive.

- Tier 1 Fines:

Up to €10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These fines apply to infringements such as:

- Failing to implement data protection by design and by default.
- Not maintaining records of processing activities.
- Not reporting data breaches to the supervisory authority and data subjects.
- Failing to conduct DPIAs where required.

- Tier 2 Fines:

Up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These fines apply to more severe infringements, including:

- Violations of the basic principles of processing, including conditions for consent.
- Infringement of data subjects' rights.
- Unauthorized international data transfers.
- Non-compliance with orders from supervisory authorities.

ii. Corrective Powers of Supervisory Authorities

The AEPD has the power to impose a range of corrective measures in addition to or instead of fines. These measures include:

- Warnings: Issuing warnings to a controller or processor when processing operations are likely to infringe provisions of the GDPR or LOPDGDD.
- Reprimands: Issuing reprimands for infringements.
- Order Compliance: Ordering the controller or processor to bring processing operations into compliance.
- Data Processing Restrictions: Imposing a temporary or definitive limitation, including a ban on processing.
- Rectification or Erasure: Ordering the rectification or erasure of personal data or restriction of processing.
- Data Protection Certification: Withdrawing a certification or ordering the certification body to withdraw it.

iii. Liability and Compensation

The LOPDGDD, in conjunction with the GDPR, allows data subjects to seek compensation for damages suffered as a result of an infringement. Controllers and processors can be held liable for any material or non-material damage caused by their processing activities.

If more than one controller or processor is involved in the processing, they may be jointly liable for the entire amount of damage.

iv. Additional Enforcement Measures

- Publicity Orders: The AEPD can order organizations to publicize their infringements and the penalties imposed. This serves as a deterrent and encourages compliance by highlighting the consequences of non-compliance.
- Cease and Desist Orders: Authorities can order organizations to stop processing personal data if they fail to comply with data protection laws.

12. Conclusion

Data protection is a critical aspect of operating a business in Spain. Compliance with the GDPR and LOPDGDD is not only a legal requirement but also a commitment to safeguarding individuals' privacy and fostering trust. By implementing robust data protection measures, conducting regular reviews, and staying informed about regulatory changes, organizations can protect personal data effectively and avoid the severe financial and reputational repercussions of non-compliance.

Understanding and adhering to data protection laws ensures that personal data is handled responsibly, protecting the rights and freedoms of individuals. It also enhances the credibility and integrity of businesses, building trust with customers and stakeholders.

— — — — — — — — —

Contact Us

Please do not hesitate to contact us at **info@agg.cat** if you have any questions on any of the matters contained or referred to in this guide. Our team of experts at AGG Lawyers and Advisors is ready to provide comprehensive support and advice to help your business navigate the complexities of data protection laws. Additionally, if you require assistance with any other matter in Spain, we are here to help.