INTERNATIONAL LAWYERS NETWORK

2025 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, 2023, 2024, and 2025, they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Table of Contents

Argentina

In Argentina, data protection is governed by comprehensive legislation aimed at safeguarding individuals' personal data. Below you will find an outline of the key aspects, including governing legislation, exploring their scope of application, requirements for data processing, rights and duties of data providers/principals, processing of children's data, regulatory authorities, and consequences of non-compliance.

Governing Data Protection Legislation

1.1. Overview of Principal Legislation

Data protection in Argentina is primarily regulated by the right to Habeas Data. This right can be found in Art. 43 of the Argentine Constitution of 1994. Although this right is enshrined in the Constitution, the implementation of protection to the personal data is regulated by the Personal Data Protection Law No. 25,326 ("Ley de Protección de Datos Personales", hereinafter "PDPL"), enacted in 2000. The PDPL is the cornerstone of Argentina's data protection regime. It aims to strike a balance between the free flow of information and individuals' right to privacy. This legislation imposes strict obligations on data controllers and data processors while affording data subjects various rights. This legislation establishes the fundamental principles and requirements for the processing of personal data in the country. It aligns with international data protection standards and provides a strong legal framework for data protection.

In recent years, several legislative initiatives have been introduced in Congress to modernize Argentina's PDPL. Three main proposals aim to update the current framework by aligning national regulations with international standards, introducing concepts such as anonymization, biometric data, automated decision-making, and profiling. These bills propose, among other aspects, expanding legal bases for data processing, strengthening safeguards for minors and public-sector data, requiring impact assessments under specific conditions, and establishing mandatory security breach notifications and differentiated sanction regimes.

Contact Us

+54 11 5278 5280

https://syls.com.ar/

jmca@syls.com.ar

Arroyo 880, 2º Piso
Buenos Aires, C1007AAB Argentina

1.2 *Additional or Ancillary Regulation, Directives, or Norms*

Complementing the principal legislation, several regulations and guidelines further detail data protection requirements. Notably, the Argentine Data Protection Authority ("Agencia de Acceso a la Información Pública", hereinafter "AAIP"), the regulatory body responsible for enforcing data protection laws in Argentina, issues resolutions and guidelines to clarify specific aspects of data protection, ensuring consistent compliance across various sectors and industries, and providing further clarity of the PDPL, especially with newer technologies. These directives help organizations understand their obligations and best practices regarding data protection.

Scope of Application

2.1. Legislative Scope

2.1.1. Definition of Personal Data

The PDPL has a broad scope of application, covering the processing of personal data within the country's borders. The PDPL discriminates in Article 2 the different types of personal data that can be found and defines each one of them. Broadly, personal data is defined as encompassing any information that allows the identification of an individual or makes them identifiable. This definition includes both direct and indirect identification criteria. Some of the law's definition of personal data encompasses a wide range of information, including but not limited to names, identification numbers, addresses, and even electronic identifiers.

2.1.2. Definition of Different Categories of Personal Data

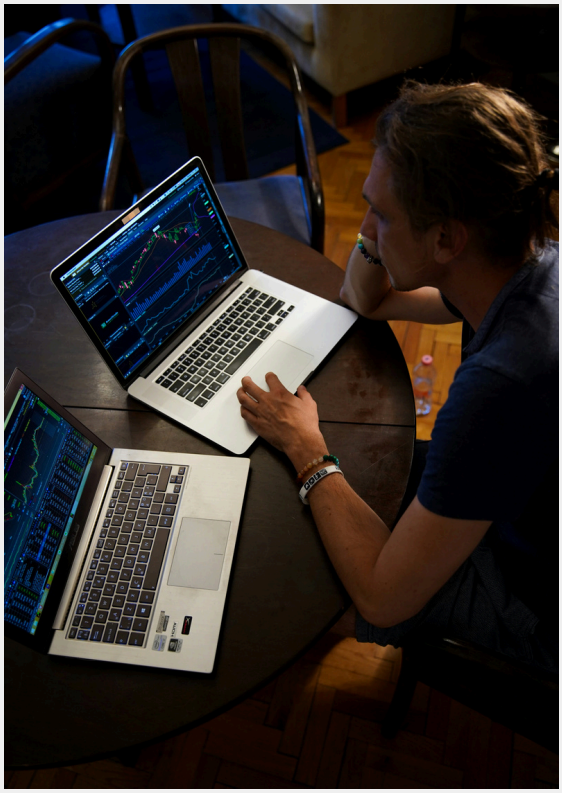
PDPL recognizes various categories of personal data, acknowledging that sensitive data, such as health records or biometric information, require special protection. Sensitive data pertains to personal information that discloses details such as racial or ethnic origin, political beliefs, religious or philosophical affiliations, moral convictions, union memberships, or data concerning one's health or sexual life. The terms 'file,' 'record,' 'database,' or 'data bank' are used interchangeably to describe organized sets of personal data subject to processing, whether electronically or otherwise, regardless of how they are created, stored, organized, or accessed

2.1.3. Treatment of Data and Its Different Categories

The PDPL regulates the processing of both personal and non-personal data, ensuring that the principles of data protection apply universally. Additionally, it outlines key definitions crucial for data processing, ensuring clarity and consistency. Data processing refers to systematic operations and procedures, electronic or not, involved in collecting, preserving, ordering, storing, modifying, correlating, evaluating, blocking, destroying, or generally managing personal data, including their transfer to third parties through various means. Regarding this definition, it addresses electronic and non-electronic data, adapting to evolving technological landscapes.

2.1.4. Other Key Definitions Pertaining to Data and Its Processing

The legislation provides key definitions related to data processing, such as data controller and data processor, ensuring clarity in roles and responsibilities within data processing activities. Computerized data pertains to personal information subjected to electronic or automated processing. Data disassociation involves processing personal data in a manner that renders the information obtained incapable of being linked to a specific or identifiable individual.



https://syls.com.ar/

Statutory Exemptions

The PDPL allows for exemptions in specific situations, such as when data processing is required by law or necessary for the performance of a contract, such as data processed for journalistic, artistic, or literary purposes, domestic activitie,s or used for public security or defense. These exemptions must align with the PDPL's overarching principles and respect individuals' rights.

3.1.Territorial and Extra-Territorial Application

The PDPL applies within Argentina's territory and extends to data processing activities that have an extraterritorial impact when data controllers or processors outside Argentina process the personal data of Argentine residents.

Legislative Framework

4.1. Key Stakeholders

- **Data Controller:** Individual or legal entity, whether public or private, who is the owner of a file, record, database, or data bank.
- **Data Processor:** Entities or individuals that process data on behalf of the data controller.
- **Data Subject:** The individual to whom the personal data belongs and is being processed.

4.2 Role and Responsibilities of Key Stakeholders

The PDPL assigns specific responsibilities to each stakeholder, emphasizing the data controller's duty to inform data subjects, obtain consent, and ensure data security. Data Controllers in Argentina must ensure compliance with the PDPPL, obtain explicit consent for data processing, and protect data subjects' rights. They are responsible for notifying data subjects about the purpose and scope of data processing. Moreover, they must register with the AAIP as data controllers as well as any database containing personal data, whether public or private.

Data Processors are required to process data strictly in accordance with the instructions provided by the Data Controller. They must also implement robust data security measures to protect the data they handle.

Data subjects in Argentina have various rights, including the right to access their data, rectify inaccuracies, and request data erasure when necessary.

Requirements for Data Processing

5.1. Grounds for Collection and Processing

Data processing must be based on lawful grounds, including consent, contractual necessity, legal obligations, vital interests, or legitimate interests pursued by the data controller. Data processing often requires the explicit and informed consent of the data subject.

Consent notices should clearly outline the purpose of data processing, and data subjects have the right to withdraw their consent at any time. Consent is a fundamental requirement, and individuals have the right to withdraw it at any time.

5.2. Data Storage and Retention Timelines

The PDPL requires data controllers to establish retention periods that align with the purpose of data processing. Data storage and retention timelines are defined in accordance with the purpose for which the data was collected. Argentina's regulations specify maximum periods for data retention and the conditions under which data can be retained.

5.3. Data Correction, Completion, Update, or Erasure of Data

Individuals have the right to request corrections or erasure of inaccurate or outdated data concerning them. Data controllers are obligated to respond to such requests promptly.

5.4. Data Protection and Security Practices and Procedures

Data protection and security practices are of paramount importance. Data controllers and processors are required to implement security measures to protect personal data from

https://syls.com.ar/

unauthorized access, disclosure, alteration, or destruction. Some examples of these security measures are encryption, access controls, and regular audits to protect personal data from breaches. These measures must be commensurate with the sensitivity of the data being processed.

5.5. Disclosure, Sharing, and Transfer of Data

Transfers of personal data to third parties require data subject consent or a legal basis.

Cross-border data transfers must adhere to data protection regulations and, in certain cases, require authorization from the AAIP, as further discussed below.

5.6. Cross-Border Transfer of Data

Cross-border data transfers are subject to specific rules and safeguards, which are in line with international data protection standards.

On January 15, 2024, the European Commission ("Commission") published its findings regarding the first review of adequacy decisions made under Article 25(6) of Directive 95/46/EC ("Directive") in 1995. In these decisions, the Commission had determined that eleven countries or territories, including Argentina, ensured an adequate level of personal data protection, allowing for the free transfer of data from the European Union (EU) to these countries or territories. With the entry into force of the EU General Data Protection Regulation (GDPR) in 2018, it was established that adequacy decisions made under the Directive would remain in effect but would be subject to review every four years. In this first review, the Commission found that the data protection frameworks in the countries and territories under review had evolved, including through legislative reforms and regulations by data protection authorities.

Regarding Argentina, the Commission emphasized the importance of the independence of the AAIP as the supervisory authority and the ratification of Convention 108+ in 2023. Additionally, it noted that a draft Data Protection Bill introduced in Congress and still subject to review could further strengthen the data protection framework in the country. As a result of its findings, the European Commission concluded that personal data transferred from the European Union to Argentina benefits from adequate protection guarantees. Consequently, such data can continue to flow freely from the EU to Argentina, maintaining the country's position at the forefront of personal data protection and facilitating greater efficiency and security in international operations.

5.7. Grievance Redressal

The PDPL mandates the establishment of grievance redressal mechanisms, enabling data subjects to exercise their rights and seek remedies in cases of non-compliance.

Rights and Duties of Data Providers/Principals

6.1. Rights and Remedies

- **Right to Withdraw Consent:** Individuals have the right to withdraw their consent for data processing at any time.
- **Right to Grievance Redressal and Appeal:** Data subjects can file complaints with the Data Protection Authority and seek judicial remedies.
- **Right to Access Information (Habeas Data):** Art. 43 of the Argentine Constitution grants individuals the right to access, update, or delete personal data held about them.
- **Right to Nominate:** Individuals can nominate a representative to exercise their data protection rights.

6.2. Duties

Data controllers and processors are duty-bound to provide accurate information, report changes, and respect the rights and privacy of others in accordance with Argentina's data protection regulations.

Processing of Children or Minors' Data

The PDPL places special emphasis on protecting the data of children and minors, requiring parental consent for data processing activities involving minors.

Regulatory Authorities

8.1. Overview of Relevant Statutory Authorities

The AAIP is the regulatory authority responsible for enforcing the PDPL, and has the power to issue resolutions and guidelines to clarify specific aspects of data protection and keep the data protection regulation updated to upcoming technologies.

8.2. Role, Functions, and Powers of Authorities

The AAIP plays a crucial role in overseeing compliance with data protection regulations. It is tasked with monitoring compliance, investigating data breaches, and issuing penalties for violations.

8.3. Role, Functions, and Powers of Civil/Criminal Courts in the Field of Data Regulation

Civil and criminal courts can be involved in data protection cases, particularly when individuals seek

legal remedies for data breaches or non-compliance with data protection laws.

Consequences of Non-Compliance

9.1. Consequences and Penalties for Data Breach

Data controllers and processors in Argentina face significant penalties and consequences for data breaches, including fines and mandatory notifications to affected data subjects. Non-compliance with data protection laws, including data breaches, can result in severe penalties, including fines, suspension of data processing activities, or data controller disqualification. The PDPL modifies some of Argentina's criminal laws (articles 117 bis and 157 bis ofthe National Penal Code) to include cases in which data controllers and processors are punished for Data breaches and Non-Compliance.

9.2. Consequences and Penalties for Other Violations and Non-Compliance

Violations of other provisions of data protection laws may also lead to penalties, depending on the severity of the violation.

Contact Us

+54 11 5278 5280

https://syls.com.ar/

jmca@syls.com.ar

Arroyo 880, 2° Piso
Buenos Aires, C1007AAB Argentina

Brazil

Introduction

The Brazilian General Data Protection Law ("LGPD"), enacted in 2018 and enforced since 2020, serves as the cornerstone of the country's data protection framework. Its primary objective is to ensure the fundamental rights of data subjects and regulate how personal data is processed by processing agents. The LGPD outlines the rights and obligations of data controllers and processors, establishes enforcement mechanisms through sanctions and inspections, and fosters overall governance of data processing activities.

Before the LGPD, data protection and privacy rights were governed by a patchwork of sector-specific laws covering areas like consumer rights, finance, healthcare, the public sector, and criminal law. Additionally, the Civil Rights Framework for the Internet ("Marco Civil da Internet"), enacted in 2014 with its accompanying decree, laid the groundwork for processing personal data online.

Governing Data Protection Legislation

2.1.Overview of principal legislation

The LGPD, Federal Law No. 13,709/2018, aims to safeguard the fundamental rights of freedom and privacy, fostering the personal development of individuals. It represents a major regulatory advancement, aligning Brazil's data protection legislation with international standards. Signed by the President on August 14, 2018, published on August 15, 2018, and taking effect on September 18, 2020, the LGPD marked a significant shift in how personal data is treated in Brazil.

Further emphasizing this importance, the protection of personal data was expressly recognized as a fundamental right in Brazil's Federal Constitution (Article 5, LXXIX) in 2022. This inclusion highlights the high level of protection and priority assigned to safeguarding personal data within the country.

Contact Us

+55 (11) 3799-8100

https://klalaw.com.br/en/home/

accesar@klalaw.com.br

Av. Brigadeiro Faria Lima, 1355
São Paulo, SP 01452-919 Brazil

2.2. Additional or ancillary regulation, directives, or norms

A key provision of the LGPD is the establishment of the Brazilian Data Protection Authority ("ANPD"). Beyond its main role in overseeing data processing and legislation adherence, the ANPD also offers comprehensive guidance and clarification on complex and important issues encountered by data controllers in their operations.

The ANPD has issued several regulations to enhance clarity and compliance within the LGPD framework, including the Regulation of the Inspection and Administrative Sanctioning Processes, specific to the ANPD's role and authority. The Authority has also issued regulations for applying the LGPD to small-scale data controllers and on the application of penalties, among others.

More recently, the ANPD issued Resolutions No. 18/241 and No. 19/242, which also mark significant developments in the Brazilian data protection framework. Resolution No. 18 provides detailed guidance on the role, responsibilities, and minimum requirements for the Data Protection Officer (DPO), while Resolution No. 19 establishes rules and safeguards for international transfers of personal data. As will be further detailed in the following sections, both resolutions bring greater specificity to key areas of data protection, offering practical guidance that enhances legal certainty and operational clarity for organizations. Moreover, they underscore the ANPD's pivotal role in the national data protection ecosystem, reinforcing its authority in setting standards and providing concrete directions for the effective and consistent application of the LGPD.

Scope of Application

3.1. Legislative Scope

The LGPD applies to any personal data processing activity carried out by individuals or legal entities, whether private or public. This applies regardless of the processing method (online or offline), the company's headquarters location, or the data's location, provided that: (i) the processing is performed in national territory; (ii) the processing activity has the purpose of offering or providing goods or services to individuals located in the national territory; (iii) the processing activities have, as purpose, the processing of data from individuals located in the national territory; or (iv) when the personal data has been collected in the national territory.

The country in which the processing agents were incorporated or have head offices, the nationality and place of residence of the data subjects, and the country where the data is located are all elements that are considered irrelevant to the assessment of whether the LGPD shall apply to a given processing activity.

3.1.1. Definition of personal data

Personal data is defined as any information related to an identified or identifiable natural person. Under the LGPD, personal data encompasses not only directly identifying information, such as names and identification numbers, but also information that, when combined or utilized in conjunction, enables the identification of an individual.

3.1.2. Definition of different categories of personal data

Sensitive personal data is classified as any personal information related to an individual's racial or ethnic origin, religious beliefs, political opinions, membership in trade unions, or religious, philosophical, or political organizations, as well as data concerning health, sexual life, and genetic or biometric details. The processing of these categories of personal data poses significant risks to an individual's fundamental rights and freedoms, necessitating a higher standard of protection under the Law.

Anonymized data refers to information about a data subject that cannot be identified, considering the use of reasonable technical means available at the time of processing. The anonymized data falls outside the scope of the Law.

3.1.3. Processing of personal data and its different categories

The LGPD mandates that the processing of personal or sensitive personal data must follow the legal bases established for each category of data, as detailed in Articles 7 and 11. Information on the legal bases can be found in Section 5.1 of this Guideline.

3.2 Statutory exemptions

The LGPD and its regulations are designed to govern the processing of personal data about identified or identifiable natural persons. Consequently, data exclusively associated with legal entities (for example, the Brazilian National Registry of Legal Entities) falls outside the purview of the legislation.

Furthermore, the LGPD does not apply to data processing that is conducted by natural persons solely for personal, non-commercial purposes, or data processed exclusively for journalistic, artistic, public security, national defense, state security, or in activities connected with the investigation and repression of crimes. Additionally, data originating from outside Brazil that is not subject to communication or shared use with Brazilian processing agents is also exempt from the scope of the LGPD.

3.3.Territorial and extra-territorial application

Article 3 of the LGPD states that any processing activity conducted by a natural person or a legal entity is subject to the law, irrespective of where the entity is located or where the data resides.

This applies if the activity meets any of the following conditions: **(i)** the processing occurs in Brazil; **(ii)** the processing aims to offer goods or services or involves handling personal data of individuals in Brazil; or **(iii)** the personal data being processed was collected in Brazil.

Consequently, due to the extraterritorial application of the LGPD, factors such as the country of incorporation or location of the processing agents' head offices, the nationality and residence of the data subjects, and the location of the data are deemed irrelevant in determining whether the LGPD applies to a specific personal data processing activity.

Legislative Framework

4.1.Key stakeholders

4.1.1 Data subject

The term 'data subject' refers to the natural person associated with the personal data being processed. Essentially, it denotes the individual who is related to the personal data.

4.1.2. Controller

The controller is defined as the "natural or legal person, whether governed by public or private law, who is responsible for decisions relating to the processing of personal data". As the primary authority, the controller decides the purposes for which personal data is processed and sets the guidelines for processors on how to handle this data processing on their behalf.

4.1.3 Processor

The processor is defined as the "natural or legal person, whether governed by public or private law, who carries out the processing of personal data on behalf of the controller". In practical terms, the processor is most often a company hired by the controller to carry out data processing following instructions provided by the controller.

Additionally, it is a common practice for processors to engage sub-processors to assist in data processing activities. Although the LGPD did not initially define this concept, the ANPD later acknowledged its legality. This recognition was made in the ANPD's 'Guidelines for Definitions of Personal Data Processors and DPO', where a sub-processor is defined as an entity 'hired by the processor to aid in processing personal data on behalf of the controller.' The Guidelines also clarify that the sub-processor maintains a direct relationship with the processor, rather than with the controller.

4.1.4 Data Protection Officer ("DPO")

The Data Protection Officer ("DPO") is designated by the controller to serve as the liaison among the controller, data subjects, and the ANPD. According to Article 41, the controller must appoint a DPO, who will oversee the data processing operations.

https://klalaw.com.br/en/home/

Complementing the provisions of the LGPD, the ANPD issued Resolution No. 18/24, which provides detailed rules on the appointment, duties, and responsibilities of the DPO, as well as the obligations of data processing agents to ensure the proper performance of this role.

The regulation requires that the DPO be formally appointed by the data processing agent through a written, dated, and signed document that clearly sets out the scope of activities. It also mandates the disclosure of the DPO's identity and contact details in a clear and easily accessible manner. Where a legal entity is appointed, the corporate name or trade name must be published, along with the full name of the individual responsible.

Processing agents are further required to provide the DPO with adequate resources, guarantee technical independence, establish effective communication channels with data subjects, and ensure direct access to decision-makers. They must also seek the DPO's input on strategic decisions involving personal data. While these measures reinforce the centrality of the DPO in compliance programs, the regulation clarifies that responsibility for compliance ultimately lies with the processing agents.

Importantly, the regulation reiterates that no formal certification, training, or registration is required to serve as a DPO. However, the DPO must be able to communicate clearly in Portuguese. In addition, the regulation addresses potential conflicts of interest, allowing the DPO to hold multiple roles or serve multiple organizations, provided that impartiality is not compromised. In such cases, the DPO must disclose the situation to the processing agent, who is then responsible for taking appropriate measures, which may include implementing safeguards, appointing another person, or declining the designation. Non-compliance with these obligations may trigger sanctions by the ANPD.

Additionally, according to ANPD's Resolution n. 2/243, small processing agents are exempt from appointing a DPO. These agents include micro-enterprises, small businesses, startups, and legal entities governed by private law, such as non-profit organizations, as defined by current legislation. This category also extends to natural persons and depersonalized private entities involved in personal data processing and undertaking the typical responsibilities of a controller. However, if a small processing agent decides not to appoint a DPO, they must establish an alternative communication channel with the data subjects to comply with the resolution.

4.2 Role and responsibilities of key stakeholders

[1] CD/ANPD RESOLUTION No. 2, OF JANUARY 27, 2022. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper

4.2.1 Controller

The Law defines the controller in Art. 5, item VI as a "natural or legal person, public or private law, to whom the decisions regarding the processing of personal data are incumbent."

The controller acts as the key processing entity responsible for setting the purposes for personal data processing.

This role involves specifying the objectives, methods, and extent of personal data handling. Under the LGPD, the controller's essential duties include: (i) adopting adequate measures to safeguard the security and confidentiality of personal data; (ii) maintaining records of processing activities ("ROPA"); (iii) providing directives to processors operating under their guidance; (iv) alerting the ANPD about any personal data breaches that require reporting; (v) conducting a Data Protection Impact Assessment ("DPIA") to secure personal data, particularly sensitive personal data, concerning its processing activities.

4.2.2 Processor

The Law defines the processor in Art. 5, item VII as a "natural or legal person, public or private law, who processes personal data on behalf of the controller." As an agent tasked with processing personal data for the controller, the processor has several responsibilities, such as: (i) adhering to the controller's instructions; (ii) maintaining the security and confidentiality of the personal data; (iii) returning or erasing the personal data upon the controller's request; and (iv) documenting the ROPA.

Under the Law, processors are jointly liable with the respective controllers for any damages arising from their processing activities if they violate legal obligations or disregard instructions from the controller. In instances of non-compliance by the processor, they will be considered, for liability purposes under the LGPD, as equivalent to the controller.

4.2.3 DPO

Under the LGPD, the DPO is responsible for accepting complaints and communications from data subjects, providing explanations, and taking appropriate action; receiving communications from the ANPD and responding accordingly; advising employees and independent contractors on the company's personal data protection practices; and performing any other duties assigned by the controller or established in complementary norms.

Resolution No. 18/24 further clarifies and expands the DPO's responsibilities, detailing their role in ensuring effective compliance. In addition to statutory duties, the DPO is expected to support the controller in key compliance activities, including reporting and documenting security incidents, maintaining records of processing activities, and preparing Data Protection Impact Assessments (DPIAs). The DPO must also advise on the adoption of technical and

organizational measures to safeguard personal data, including measures related to international data transfers, and guide employees, contractors, and other relevant stakeholders on best practices for personal data protection, reinforcing organizational awareness and accountability.

Importantly, the resolution emphasizes that, despite the DPO's central role in promoting compliance, the DPO is not personally liable before the ANPD for the lawfulness of the controller's processing activities, as ultimate responsibility remains with the data processing agents themselves.

Requirements for Data Processing

5.1. Grounds for collection and processing

The LGPD provides that personal data processing activities carried out by entities may only be performed when relying on the following legal basis:

(i) when the data subject has consented to the processing;

(ii) or the compliance with legal or regulatory obligations by the controller;

(iii) by the public administration, for the processing and shared use of data necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements, or similar instruments, subject to the provisions of Chapter IV of this Law;

(iv) for carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data;

(v) when necessary for the execution of a contract or preliminary procedures relating to a contract to which the data subject is a party;

(vi) for the regular exercise of rights in judicial, administrative, or arbitral proceedings;

(vii) for the protection of life and physical integrity of the data subject or third parties;

(viii) for the protection of health, in procedures performed by professionals of the health area or by sanitary entities;

(iX) when necessary to comply with the legitimate interests of the controller or of a third party, except when the fundamental rights and freedoms of the data subject prevail; and

(x) for the protection of credit.

The art. 11 of the LGPD states that the processing of **sensitive personal data** can only be carried out:

(i) with the express consent of the data subject or person responsible, for specific purposes or;

without the consent of the data subject, in cases where it is indispensable for:

(ii) compliance with a legal or regulatory obligation by the controller;

(iii) shared processing of personal data necessary for the execution, by the public administration, of public policies provided for in laws or regulations;

(iv) for studies carried out by research bodies, guaranteeing, whenever possible, the anonymization of sensitive personal data;

(v) regular exercise of rights, including in contracts and in judicial, administrative, and arbitration proceedings;

(vi) protection of the life or physical safety of the data subject or a third party;

(vii) protection of health, exclusively in procedures carried out by health professionals, health services, or health authorities; or

(viii) guaranteeing the prevention of fraud and the security of the data subject in processes of identification and authentication of registration in electronic systems.

Remarks on Consent: The LGPD defines consent as a freely given, informed, and unambiguous indication that the data subject agrees with the processing of their personal data for informed purposes. Consent must always be given in writing or by other means that evidence the effective manifestation of the data subject's free will, always under a clause separate from other contractual clauses and shall relate to determinate purposes, provided that any generic consent shall be deemed null.

The data subject may, at any time, revoke their consent through a free and facilitated procedure that must be made available by the controller.

5.2 *Data storage and retention timelines*

Article 165 of the LGPD stipulates that personal data processing must cease upon the occurrence of any of the following conditions:

(i) the purpose for processing the personal data has been achieved, or the data is no longer necessary or relevant for that specific purpose; (ii) the designated processing period concludes; (iii) the data subject requests the termination of processing, including as part of their right to withdraw consent, while considering public interest; or (iv) the ANPD mandates cessation due to a breach of the LGPD's regulations.

The LGPD mandates that, following the conclusion of personal data processing activities, the personal data must be deleted within the operational and technical constraints of these activities. However, personal data retention is permitted under specific conditions: **(i)** to fulfill a legal or regulatory obligation by the controller; **(ii)** for research purposes by a research entity, ensuring anonymization of the personal data whenever possible; **(iii)** for transfer to a third party, subject to adherence to the LGPD's data processing requirements; or **(iv)** for the controller's exclusive use, without third-party access, provided the data is anonymized.

5.3 *Data correction, completion, updating, or erasure of data*

As established in Section 6.1, Article 18 of the LGPD grants data subjects different rights regarding their personal data. Among these, individuals have the right to request that the controller correct any incomplete, inaccurate, or outdated personal data at any time upon their request.

5.4 *Data protection and security practices and procedures*

The LGPD mandates that controllers and processors implement technical and administrative safeguards to protect personal data against unauthorized access, as well as against accidental or illegal destruction, loss, alteration, disclosure, or any other form of improper processing.

Moreover, the Law encourages the development and implementation of best practices and governance frameworks by these entities. This encompasses addressing organizational conditions, operational protocols, internal procedures (including handling data subject requests), security policies, technical standards, specific responsibilities for those engaged in processing activities, educational initiatives, internal monitoring, and mechanisms for mitigating risks.

In this context, the ANPD is empowered to define minimum technical standards for data security and confidentiality. Reflecting this, in 2021, the ANPD released the Information Security Guide for Small Processing Agents to outline a range of security measures tailored to small-scale agents.

5.5 Cross-border transfer of data

Article 33 of the LGPD specifies the conditions under which international data transfer is permitted, including: **(i)** to entities in countries or international organizations that offer a level of personal data protection comparable to the LGPD;

(ii) when the controller demonstrates adherence to LGPD principles and data subject rights through specific agreements or mechanisms like standard data protection clauses, corporate rules, or codes of conduct approved by the ANPD; (iii) for international legal cooperation among public intelligence or law enforcement agencies; (iv) to protect the life or physical safety of the data subject or others; (v) with authorization from the ANPD; (vi) under international cooperation agreements; (vii) for executing public policies or services; (viii) with explicit consent from the data subject, clearly informed about the transfer's international aspect; and (ix) to meet the requirements in items II, V, and VI of Article 7.

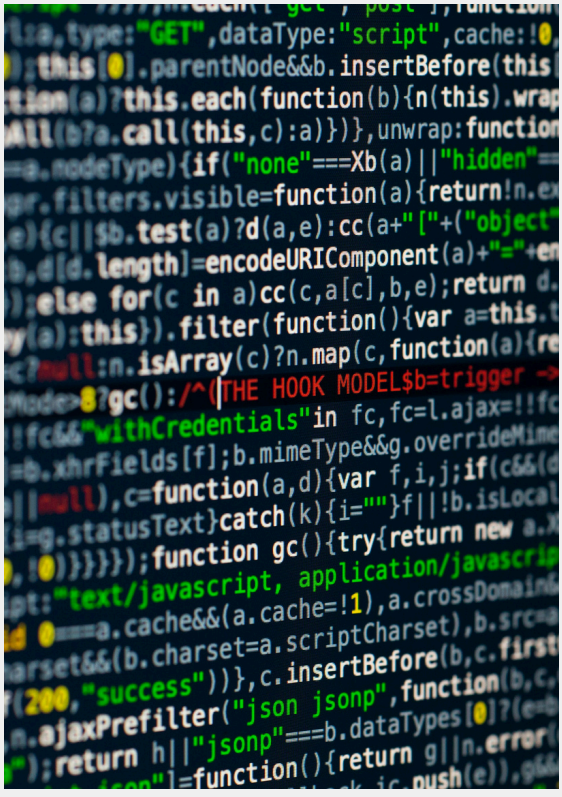
Complementing these provisions, the ANPD issued Resolution No. 19/24, which regulates international data transfers and defines the content of Standard Contractual Clauses, as provided under the LGPD. The resolution aims to ensure legal certainty and protect the rights of data subjects, regardless of where their personal data is processed. It defines an international transfer of personal data as any operation in which a data exporter transfers personal data to a data importer, requiring the identification of the processing agents involved in the transfer.

Resolution No. 19/24 establishes that international data transfers are permitted only when based on a legal basis under the LGPD and supported by one of the following mechanisms:

- **Countries with an adequate level of protection**: Transfers to countries or international organizations recognized by the ANPD as providing a level of protection comparable to the LGPD.
- **Standard Contractual Clauses (SCCs):** SCCs may be incorporated either in a dedicated contract solely governing international transfers or through an addendum to an existing agreement. Existing contracts must be updated within 12 months of the regulation's publication. The ANPD may also recognize equivalent SCCs from other jurisdictions if they are compatible with the LGPD.
- **Specific Contractual Clauses:** Controllers may implement tailored clauses to ensure full compliance with LGPD principles and data subject rights when SCCs cannot be applied due to exceptional circumstances.
- **Global Binding Corporate Rules:** Applicable to multinational corporate groups, subject to ANPD approval, specifying the details of transfers, categories of data, involved entities, purposes, responsibilities, and communication channels with data subjects.
- **Seals, certifications, and codes of conduct:** These mechanisms are permitted provided they ensure adherence to LGPD principles and safeguard the rights of data subjects.

- **Specific contexts under Article 33, items III–IX:** Including international legal cooperation, protection of life or physical safety, execution of public policies, explicit consent, legal or regulatory obligations, and contractual necessities.

The regulation emphasizes that controllers must verify the characterization of any international transfer, ensure transparency, and provide clear information to data subjects regarding the purpose, destination countries, and security measures applied. Both controllers and processors are responsible for



adopting effective measures to comply with the LGPD, taking into account the risk level of the processing and the transfer mechanism employed.

https://klalaw.com.br/en/home/

Rights and Duties of Data Providers/Principals

6.1 Rights and remedies

The LGPD grants data subjects the following rights, among others:

a) obtain confirmation about the existence of processing activities of their data;

b) access the data that is subject to processing;

c) the right to correct incomplete, inaccurate, or outdated data;

d) have unnecessary or excessive data anonymized, blocked, or eliminated;

e) portability of data to a different provider of goods or services;

f) eliminate data that is processed based on their consent;

g) obtain information about public and private entities with which their data is shared;

h) obtain information on the possibility of not giving their consent and also on the consequences of such an option;

i) revoke their consent; and

j) petition against the controller before the ANPD as well as before consumer defense bodies, where applicable.

Importantly, Article 43 of the LGPD outlines scenarios in which processing agents may be exempt from liability. These exemptions apply if the processing agents can demonstrate **(i)** that they did not perform the personal data processing activity assigned to them; **(ii)** that they did perform the assigned processing activity, but there was no violation of data protection legislation; or **(iii)** that the damage is solely due to the fault of the data subject or a third party.

9.2 Consequences and penalties for other violations and non-compliance

Article 52 of the LGPD outlines a comprehensive range of administrative sanctions for data processing agents found in violation of its regulations, emphasizing the law's commitment to enforcing data protection principles. The potential sanctions include: **(i)** warning, with a deadline for adopting corrective measures; **(ii)** fines up to two percent (2%) of the turnover of the private legal entity, group, or conglomerate in Brazil for the last financial year, excluding taxes, with a cap of fifty million reais (R$50,000,000.00) per infraction; **(iii)** daily fines, subject to the total limit of fifty million reais (R$50,000,000.00); **(iv)** publicization of the infringement after its occurrence has been duly ascertained and confirmed; **(v)** blocking of the personal data to which the infringement relates until the activity is regularized; **(vi)** deletion of the personal data to which the infringement relates; **(vii)** partial suspension of the operation of the database to which the infringement relates for a maximum period of six (6) months, extendable for the same period, until the controller regularizes the personal data processing activity; **(viii)** suspension of the personal data processing activity to which the infringement relates for a maximum period of six (6) months, extendable for an equal period; and **(ix)** partial or total prohibition of the exercise of activities related to personal data processing.

The LGPD ensures that the application of these sanctions considers a variety of factors, such as the severity and nature of the breaches; good faith of the breaching party; economic condition of the breaching party; extent of the damage; and cooperation of the breaching party with the authorities.

Conclusion

Brazil has taken significant steps in data protection regulation with the enforcement of the LGPD in recent years. This landmark legislation serves as a cornerstone for protecting personal data, ensuring compliance with key principles, and aligning Brazil with international privacy and data protection standards. The ANPD plays a crucial role in this landscape, actively enforcing the LGPD's requirements for data controllers and processors.

This collaborative effort between the legislative framework and the ANPD marks a major advance in Brazil's approach to data protection. This positions the country as a player in the global dialogue on data protection standards.

deletion of the personal data to which the infringement relates; (vii) partial suspension of the operation of the database to which the infringement relates for a maximum period of six (6) months, extendable for the same period, until the controller regularizes the personal data processing activity; (viii) suspension of the personal data processing activity to which the infringement relates for a maximum period of six (6) months, extendable for an equal period; and (ix) partial or total prohibition of the exercise of activities related to personal data processing.

The LGPD ensures that the application of these sanctions considers a variety of factors, such as the severity and nature of the breaches; good faith of the breaching party; economic condition of the breaching party; extent of the damage; and cooperation of the breaching party with the authorities.

Contact Us

+55 (11) 3799-8100
https://klalaw.com.br/en/home/
accesar@klalaw.com.br
Av. Brigadeiro Faria Lima, 1355
São Paulo, SP 01452-919 Brazil

Canada

Introduction

As a federal state with law-making powers shared between federal and provincial/territorial governments, Canada has both federal and provincial/territorial privacy laws that govern the private and public sectors (as of November 2025, there are over 30 different privacy laws federally, provincially and territorially in Canada).

Canada's two federal privacy laws are:

- the Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (PIPEDA); and
- the Privacy Act, R.S.C., 1985, c. P-21 (the Privacy Act).

Currently, three provinces have legislation that is deemed substantially similar to PIPEDA:

- the Personal Information Protection Act, SA 2003 c P-6.5 (Alberta);
- the Personal Information Protection Act, SBC 2003, c 63 (British Columbia); and
- an Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 , as amended by Law 25, an Act to Modernize Legislative Provisions as regards the Protection of Personal Information.

The Privacy Commissioner of Canada (the Commissioner) oversees PIPEDA and the Privacy Act. The Commissioner is an independent agent of Parliament and heads the Office of the Privacy Commissioner of Canada (the OPC).

While PIPEDA regulates the private sector and generally applies across Canada, the Privacy Act is a limited statute in that it applies only to federal government institutions and Crown corporations.

This chapter will highlight the key provisions of PIPEDA, as the principal legislation for private sector privacy law in Canada. The chapter will not address provincial privacy laws, public sector privacy laws, or personal health information laws at the federal or provincial levels.

Contact Us

(416) 864 9700
https://www.foglers.com/
lprokopich@foglers.com
40 King Street West, Suite 2400
Scotia Plaza
Toronto, ON M5H 3Y2 Canada

Businesses that operate in Alberta, British Columbia or Quebec should consider how the applicable provincial privacy statutes may affect their operations, as the statutes differ from PIPEDA in certain respects.

Governing Data Protection Legislation

1.1. Overview of principal legislation

Enacted in 2001, PIPEDA regulates the collection, use and disclosure of personal information by organizations in the course of commercial activities in Canada. It aims to balance an individual's right to privacy with an organization's need to collect, use, and disclose personal information. PIPEDA applies regardless of the technology employed.

1.2. Upcoming or proposed legislation

- The Federal Government has also proposed Bill C-8, legislation aimed at preventing cybersecurity incidents.
- There are ongoing provincial privacy law reform initiatives in Ontario, British Columbia and Alberta.

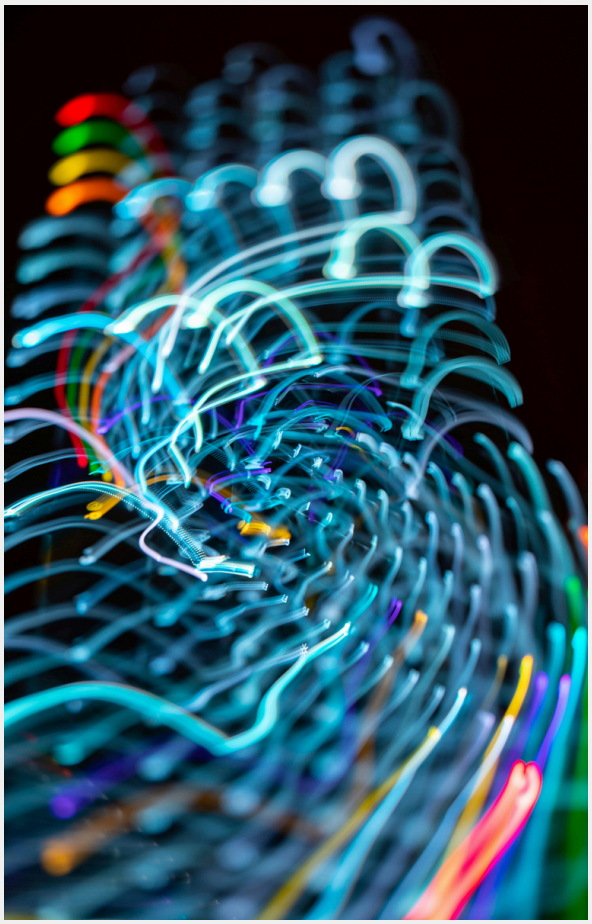
Consumer Privacy Protection Act (CPPA)

If enacted, the CPPA would replace PIPEDA. It differs from PIPEDA in several key respects, some of which will be highlighted in this chapter.

If enacted, Bill C-8 (An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts) would amend the Telecommunications Act and create the new Critical Cyber Systems Protection Act (CCSPA):

Part One: Telecommunications Act

If enacted, Part One of Bill C-8 would amend the Telecommunications Act to explicitly identify the security of



Canada's telecommunications system as a core objective of national telecommunications policy. It would grant the Governor in Council and the Minister of Industry expanded powers to protect Canada's telecommunications infrastructure, including the authority to prohibit telecommunications service providers from using certain products or services, mandate the removal of specified equipment from their networks or facilities and require providers to implement designated security measures.

Providers required to comply with orders would not be entitled to recovery for losses incurred. Enforcement would include both administrative monetary penalties and criminal prosecution and imprisonment.

Part Two: Critical Cyber Systems Protection Act

If enacted, Part Two of Bill C-8 would enact the CCSPA, which would establish new cybersecurity obligations for designated operators responsible for vital services or systems within the federal sector. In essence, the CCSPA would establish a proactive cybersecurity framework that places ongoing responsibility on operators to manage risks before incidents occur, rather than relying solely on reactive post-incident measures.

As currently drafted, Schedule 1 identifies telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems within federal jurisdiction, banking systems, and clearing and settlement systems as the vital services and systems that would fall under the CCSPA.

Under the CCSPA, designated operators would be required to:

- Establish, implement and maintain a cybersecurity program within 90 days of being designated, notify the appropriate regulator once the program is in place and provide the regulator with a copy of the program;
- Identify, manage and mitigate risks arising from third-party service providers and supply-chain dependencies;
- Report cybersecurity incidents to the Communications Security Establishment within 72 hours and notify the relevant regulator;
- Comply with confidential cybersecurity directions issued by the Governor in Council; and
- Maintain all required cybersecurity records in Canada, in the manner and location prescribed by regulation.

The CCSPA would grant regulators broad authority to verify compliance. Its enforcement framework would include both administrative and criminal measures. Administrative penalties could involve monetary fines, compliance agreements and personal liability for directors and officers, while criminal offences could lead to substantial fines or imprisonment for up to five years for serious violations.

Scope of Application

2.1. Legislative Scope

PIPEDA applies to organizations that collect, use, or disclose personal information in the course of commercial activities, unless that organization is exempted. PIPEDA defines commercial activity as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership, or other fundraising lists.

PIPEDA also applies to federal works, undertakings, or businesses (FWUBs), such as airports, airlines, banks, inter-provincial and international transportation companies, telecommunications companies, and radio and television broadcasters. PIPEDA's coverage here extends to personal information about FWUBs' employees and applicants for employment (notably, such coverage does not extend to employees of organizations that are not FWUBs).

PIPEDA does not apply to charities and non-profit organizations, as long as they do not engage in commercial activities. Finally, PIPEDA lists organizations to which it specifically applies to in Schedule 4; only the World Anti-Doping Agency is listed.

2.1.1. Definition of personal information

Personal information is defined as information about an identifiable individual. PIPEDA does not define "individual" but the OPC has indicated that "individual" means a natural person.

Personal information includes any factual or subjective information, recorded or not about an identifiable individual. This includes information collected in any form (e.g., in electronic or other formats).

2.1.2. Different categories and types of personal data

Sensitive information is not defined in PIPEDA. However, sensitivity is tied to consent and safeguarding principles, and is a factor in determining whether a data breach creates a real risk of significant harm.

While some personal information is generally considered sensitive (e.g., health information), sensitivity can also depend on the context. Sexual orientation, ethnic and racial origins, children's information, religious information, political affiliations, genetic and biometric data, and/or information affecting a person's reputation have all been considered sensitive information.

Other examples of types of personal information are:

- photographs and video surveillance;
- facial recognition and facial detection;
- location data (e.g., GPS and RFID); and
- employee and employee work product information.

2.1.3. Treatment of data and its different categories

Organizations are expected to comply with PIPEDA when dealing with personal information and use a higher level of care when the information is sensitive in nature.

Information that does not identify an individual or is anonymous is generally not subject to PIPEDA. PIPEDA does not explicitly address personal information that has been de-identified, however, it also does not distinguish de-identified from anonymized information.

2.2. Statutory exemptions

The following are exempt from PIPEDA:

- personal information that is handled by the federal organizations listed under the Privacy Act;
- provincial or territorial governments and their agents;
- business contact information that is collected, used, or disclosed solely for the purpose of communicating with that person in relation to their employment;
- an individual's collection, use or disclosure of personal information strictly for personal purposes; and
- an organization's collection, use or disclosure of personal information solely for journalistic, artistic, or literary purposes.

2.3. Territorial and extra-territorial application

PIPEDA applies across Canada unless an organization is operating in a province with legislation that has been deemed substantially similar to PIPEDA. PIPEDA may also apply to organizations outside Canada if there is a real and substantial connection to Canada.

Legislative Framework

3.1.Key stakeholders

Data Controller: PIPEDA does not use this term, however, organizations subject to PIPEDA that collect, use, or disclose personal information in the course of commercial activities are akin to "data controllers".

Data Processors: PIPEDA does not use this term. That said, while not explicitly defined, PIPEDA refers to "service providers" which are akin to "data processors".

Data Subject: PIPEDA does not use this term. PIPEDA protects the personal information of individuals who are akin to "data subjects".

Organization: PIPEDA defines this term as an association, a partnership, a person, and a trade union.

3.2. Role and responsibilities of key stakeholders

Schedule A to PIPEDA sets out the ten fair information principles that organizations must comply with:

1. Accountability

- Designate responsible persons for privacy law compliance.
- Ensure personal information transferred to third parties for processing has a comparable level of protection (e.g., via contractual or other measures).
- Implement privacy policies and procedures, which include procedures to protect personal information, training employees, and processes for responding to complaints or inquiries.

2. Identifying Purposes

- Document the purposes for which personal information is collected. The purposes should be specified at or before the time of collection. New purposes require fresh consent.

3. Consent

- Acquire consent for the collection, use and disclosure of personal information, unless an exemption applies.

4. Limiting Collection

- Limit the collection of personal information to that which is necessary to fulfil the identified purposes. Collecting personal information indiscriminately is prohibited. Personal information may only be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

- Develop guidelines and implement procedures with respect to the retention of personal information, including setting minimum and maximum retention periods.

6. Accuracy

- Maintain personal information sufficiently accurate, complete, and up to date, to minimise the possibility that inappropriate information may be used to make a decision about the individual.
- Routine updating of personal information is prohibited unless this process is necessary to fulfil the purposes for which the information was collected.

7. Safeguards

- Implement physical, organizational, and technological safeguards.

8. Openness

- Safeguard personal information against loss or theft, unauthorised access, disclosure, copying, use, or modification.
- Protect personal information with safeguards appropriate to the sensitivity of the information, thus more sensitive information should be safeguarded with a higher level of protection.

https://www.foglers.com/

- Ensure employees are made aware of the importance of maintaining the confidentiality of the personal information.

9. Individual Access

- Provide access to an individual to their personal information.

10. Challenging Compliance

- Put in place procedures to receive and respond to complaints or inquiries about organizations' personal information handling practices. All complaints must be investigated. If the complaint is justified, the organization must act appropriately to address the situation.

In addition to the ten fair information principles, there are compliance requirements mandated by PIPEDA:

- PIPEDA has mandatory breach reporting to both individuals and the OPC where there is a real risk of significant harm to individuals. It also has mandatory record keeping requirements for all breaches; and

- PIPEDA includes anti-spam provisions that target email address harvesting and the illicit access of another person's computer systems to collect personal information.

Requirements for Data Processing

4.1. Grounds for collection and processing

Consent (which may be express or implied, in writing or oral) is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which they are consenting. Failure to convey the purposes for collecting may render consent meaningless.

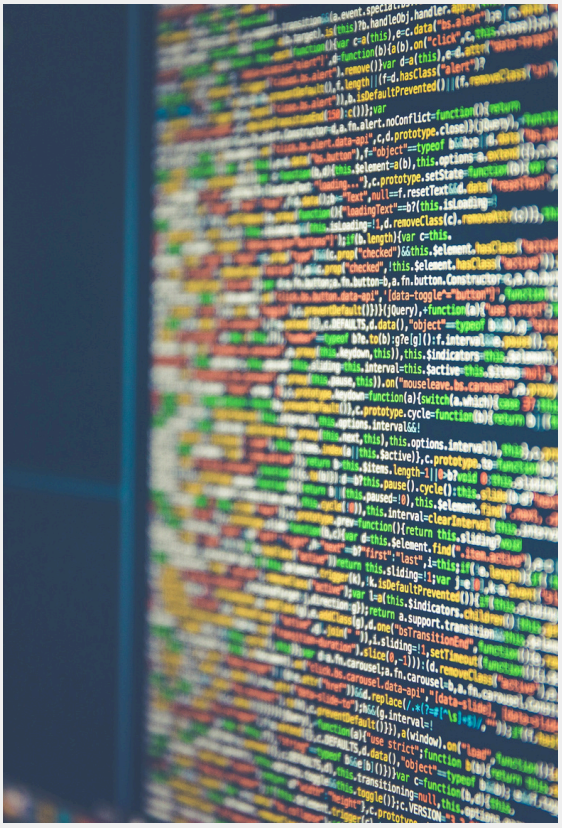
4.2. Data storage and retention timelines

PIPEDA mandates retaining personal information only as long as necessary to fulfil its purpose. Once the information no longer fulfils that purpose, it should be destroyed, erased, or made anonymous. Personal information used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

PIPEDA provides limited direction on the destruction of personal information. Organizations must develop their own guidelines that govern the disposal or destruction of personal information.

4.3. Data correction, completion, updating or erasure

Personal information about an individual must be accurate, complete and up to date. Organizations must respond to requests to amend personal information about individuals. An amendment may involve the correction, deletion or addition of information.



If requested, organizations must also be able to provide an account of the third parties to which the information has been disclosed. Access must be provided for free or a minimal fee, within a reasonable time.

4.4. Data protection and security practices and procedures

PIPEDA requires organizations to implement appropriate safeguards against unauthorized access or modification of personal information. It mandates appointing privacy officer(s) to be accountable for ensuring compliance. The name, title and contact information of the privacy officer(s) must be readily available as they must act as the point of contact for individuals with compliance concerns.

4.5. Disclosure, sharing and transfer of data

Organizations transferring data to service providers must ensure compliance by third parties. Contractual safeguards and monitoring can ensure that service providers are also compliant with

Individuals must receive notice about a potential transfer of information outside of Canada, but the individual's consent to the transfer is not required.

Rights of Data Subjects

5.1. Rights and remedies

PIPEDA provides individuals with the following rights regarding their personal information:

1. To be informed

- Organizations must inform the individual about the information collected, used, and disclosed and the purpose for such activities.

2. To withdraw consent

- May withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Organizations must inform the individual of the withdrawal's implications.

3. To access information

- Access their personal information.
- Upon request, access must be provided for free or at a minimal fee, within a reasonable time. PIPEDA provides for time limits, costs, and exceptions to access outside the principles concerning access.

4. To correction / rectification

- Request the correction, deletion, or addition of information. If appropriate, the amended information shall be transmitted to third parties that have access to the information in question.

5. To grievance redressal and appeal

- File a complaint about an organization's policies and practices relating to the handling of personal information. Organizations must investigate all complaints and must take appropriate corrective measures if justified.
- Individuals who pursue the internal complaint process may subsequently pursue an external process with the OPC. While not a precondition for OPC recourse, exhaustion of internal complaint processes may be required in certain cases.

Collecting and Processing the Personal Data of Children or Minors

PIPEDA does not have a section specific to minors, although Clause 4.3 of Schedule A to PIPEDA does say "seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated".

The OPC has interpreted and enforced PIPEDA in ways that establish privacy protections for minors. For example, the OPC has provided guidance stating that the information of minors will be considered particularly sensitive. It also has a general rule that meaningful consent cannot be obtained from minors under the age of 13.

Regulatory Authorities

7.1. Overview of relevant statutory authorities

The Commissioner is an independent agent of Parliament and heads the OPC.

7.2. Role, functions, and powers of authorities

The OPC has the authority to investigate complaints made under PIPEDA and can issue findings, express opinions regarding complaints, and make recommendations where it believes a violation has occurred.

Complaints can be initiated by an individual or by the Commissioner if satisfied that there are reasonable grounds to investigate a matter.

Complaints can be declined or discontinued for various reasons, including:

- the complaint could be more appropriately dealt with by another procedure under Canadian law;
- the organization has provided a fair and reasonable response to the complaint; or
- the matter is already the object of an ongoing investigation.

The Commissioner has an array of investigative powers but no ability to impose administrative monetary penalties. At the end of an investigation, the Commissioner may make recommendations in a Report of Findings and make that report public.

Investigation respondents and complainants both have recourse to the Federal Court of Canada. In some cases, the Court has awarded damages for breaches of PIPEDA. However, these awards have been well below penalties issued in Europe under the General Data Protection Regulation or in the United States under the Federal Trade Commission Act.

https://www.foglers.com/

7.3. Role, functions, and powers of civil/criminal courts in the field of data protection

Individuals may commence litigation against organizations breaching privacy statutes. PIPEDA does not currently establish a private right of action, however, non-compliance may result in claims under contract law and/or tort law, such as negligence, breach of contract and privacy torts. In Ontario (and not necessarily in other provinces or territories in Canada), there are four privacy torts:

- intrusion upon seclusion;
- public disclosure of embarrassing private facts;
- appropriation of a person's name or likeness; and
- publicity placing a person in a false light.

The criminal courts do not play a role in enforcing or prosecuting under PIPEDA.

Consequences of non-compliance

8.1. Consequences and penalties for a data breach

Section 28 (1) of PIPEDA states that organizations that knowingly fail to report and maintain records of every security breach that could result in a real risk of significant harm to an individual could be found guilty of:

(a)An offence punishable on summary conviction and liable to a fine not exceeding $C10,000; or

(b)An indictable offence and liable to a fine not exceeding $C100,000.

8.2. Consequences and penalties for other violations and non-compliance

Section 28(1) of PIPEDA also applies to the following offences:

- obstructing the Commissioner or the Commissioner's delegate in the investigation of a complaint or in the conduct of an audit;
- failing to retain personal information that is the subject of an access request for so long as is necessary to enable the requester to exhaust any recourse available under PIPEDA; and
- disciplining or otherwise disadvantaging an employee who has acted in good faith and based on reasonable belief with a view to securing compliance with PIPEDA.

https://www.foglers.com/

Conclusion

Canada's privacy landscape, governed by federal and provincial/territorial laws, reflects a commitment to balancing individual privacy rights with organizational needs in the digital age. While PIPEDA has served as the cornerstone of private-sector privacy regulation for over twenty years, recent legislative initiatives such as Bill C-8 and Quebec's Law 25 underscore the increasingly complex privacy landscape that continues to develop in Canada.

The European Commission renewed Canada's adequacy status on January 15, 2024. An adequacy ruling allows data controllers or data processors to transfer personal data to a country outside the European Union ("EU"). The ruling signifies that the receiving country's privacy laws have an adequate level of protection for personal data. When a country is granted adequacy status, personal data can flow to and from the EU

without the need for additional safeguards. The EU report specifically highlights and recommends enshrining protections that have been developed at a sub-legislative level in Canada to enhance legal certainty. The report also mentions that recent legislative developments can further strengthen the Canadian privacy framework in a positive light.

Authors

Fogler, Rubinoff LLP (FR) is an agile, resourceful, and entrepreneurial mid-sized Canadian law firm based in Toronto, Ontario with over 130 lawyers spanning more than 20 practice areas (including Privacy, Data Governance and Cyber Security) across many industries.

The authors acknowledge, with thanks, the help of FR's articling student, **Andrea Reid**, in preparing this chapter.

Lori Prokopich is a business and finance law partner at FR. She regularly advises clients on complex commercial contracts and general corporate matters. Her practice includes privacy and data protection matters in transactions and commercial arrangements as well as evolving regulatory requirements and best practices for privacy and data governance. Lori is a graduate of University of Toronto Faculty of Law and Osgoode Hall Law School (LL.M., Securities Law).

Contact Us

(416) 864 9700

https://www.foglers.com/

lprokopich@foglers.com

40 King Street West, Suite 2400
Scotia Plaza
Toronto, ON M5H 3Y2 Canada

Security practice group. He acts for a range of clients (including businesses, trade associations, civil society, and governments) with respect not only to what the law is but how it should be modernized.

Ronald Davis is a litigation and privacy law partner at FR. He has appeared at all levels of court, including the Supreme Court of Canada and the Court of Appeal for Ontario. Ron is a cum laude University of Ottawa Common Law en français graduate. He taught at the Law Society of Ontario's Bar Admission Course for a decade. He has edited and written over 50 articles and books on varied topics and holds a PhD in French linguistics from the University of Toronto, where he was an Assistant Professor for five years.

Roberto De Pasquale is a partner in the firm's business law group. He is developing a corporate commercial practice focused on mergers, acquisitions and corporate finance. He regularly helps companies navigate complex regulatory issues, particularly in the privacy space. Roberto is a graduate of Western University's Ivey Business School and Western Law.

China

Introduction

China's legal framework for privacy and data protection is comprehensive, built upon a layered system of laws and regulations. At its core are the "Three Fundamental Laws": the Cybersecurity Law ("CSL"), the Data Security Law ("DSL"), and the Personal Information Protection Law ("PIPL"). The Three Fundamental Laws are further elaborated and supplemented by specialized regulations.

Beyond the special legislation on data protection, other laws also contribute to privacy and data protection. Notably, the Civil Code includes provisions consistent with the Three Fundamental Laws, strengthening the legal foundation. Data protection statutes are also scattered in other specialized regulations, including the Criminal Law, the Consumer Protection Law, the E-commerce Law, and rules regulating technologies such as AI and facial recognition.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The CSL came into effect on June 1, 2017, becoming the first national legislation to address data privacy protection in China. The principles and general obligations regarding personal data protection are laid down in the CSL.

The DSL came into force on September 1, 2021. The DSL aims to regulate data processing activities (including personal data), guarantee data security, and promote the development and utilization of data.

The PIPL went into effect on November 1, 2021, becoming the first national law on personal data protection in the PRC. The PIPL aims to protect the rights and interests of personal data, regulate personal data processing activities, and promote reasonable use of personal data. The PIPL acts as an enhancement and clarification of China's earlier personal data laws and regulations, not as a replacement.

Contact Us

+86 21 3135 8701

www.llinkslaw.com

david.pan@llinkslaw.com

19F, ONE LUJIAZUI, 68 Yin Cheng Road Middle,
Shanghai 200120 P.R.China

2.2. Additional or ancillary regulation, directives, or norms

In addition to the Three Fundamental Laws, China's data protection framework also encompasses specialized regulations, general laws, and regulations. These include, non–exhaustively:

(1) Specialized Regulations

- The Administrative Measures for Personal Information Protection Compliance Audits, effective from May 1, 2025. It provides requirements and guidelines for conducting compliance audits of personal data processing activities.

- The Regulations on Facilitating and Regulating the Cross–border Data Flows, effective from March 22, 2024. It aims to streamline the cross-border data transfer process by relaxing certain compliance requirements and detailing specific scenarios where data transfers are exempt from security assessments, standard contract filings, or personal data protection certifications, thereby simplifying outbound data flows for companies.

- The Regulations on the Protection of Minors in Cyberspace, effective from January 1, 2024. It aims to create a cyberspace environment conducive to minors' physical and mental health development while safeguarding their legitimate rights and interests. It comprehensively governs the collection, use, and storage of minors' personal data, mandating specific requirements such as obtaining guardian consent and prohibiting the forced provision of unnecessary personal data.

- The Measures for the Standard Contract for Outbound Transfer of Personal Information, effective from June 1, 2023. It offers a key compliance pathway for cross-border data transfers, allows Personal Data Processors (see following section 3.1.4 for definition) to transfer data abroad by entering into a standard contract with the overseas recipient, and specifies the mandatory clauses and filing requirements for such contracts.

(2)General Laws and Regulations

- The Civil Code, effective from January 1, 2021. It provides a fundamental legal basis for protecting natural persons' personal data and defines civil liabilities for infringements.

- The Criminal Law, the latest amendments of which came into effect on March 1, 2021. It imposes criminal liability for crimes infringing on citizens' personal data.

China has also formulated specialized laws and regulations regarding the protection of personal data in certain regulated industries and sectors, such as healthcare, financial services, telecommunications, and automotive.

(3)National Standards

Non-mandatory national standards and guidelines also contribute as valuable references for personal data protection practices, such as the national standard Information security technology—Personal information security specification (GB/T 35273-2020).

Scope of Application

3.1. Legislative Scope

3.1.1. Definition of personal data

According to Article 4 of the PIPL, personal data/data refers to information related to identified or identifiable natural persons recorded by electronic or other means, excluding information that has been anonymized.

3.1.2. Definition of different categories of personal data

Under the PIPL, sensitive personal data is a special category of personal data that requires a higher level of protection. Sensitive personal data is defined as personal information/data that is likely to result in damage to the personal dignity of any natural person or damage to his/her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts, as well as the personal data of minors under the age of 14.

Certain national standards provide specific examples of sensitive personal data, such as location information and criminal records. However, these examples are only for reference. To identify whether certain information will be considered as sensitive personal data, one shall always focus on the processing context, the impact on personal data subjects, and conduct a case-by-case analysis.

3.1.3. Treatment of data and its different categories

(1) Regulation of personal and non-personal data

Among the Three Fundamental Laws, the PIPL specifically regulates personal data, setting forth principles and requirements that apply to the processing (collection, storage, use, processing, transmission, provision, disclosure, and deletion) of personal data.

For example, under the PIPL, informed consent is the primary basis for processing personal data. Before processing an individual's personal data, the Personal Data Processor shall ensure that the individual clearly agrees to the processing after having been fully informed. Separate consent is required in certain situations, which means a consent must be given explicitly for a specific activity (e.g., processing sensitive personal data, collecting data from minors under 14) rather than being part of a general consent. Besides, the PIPL does allow for some other legal basis to process personal data without consent.

Broader in scope, CSL and DSL also regulate non-personal data.

(2) Regulation of electronic and non-electronic data

Under China's data protection framework, the definition of "data" generally encompasses both electronic and non-electronic forms. For instance, the PIPL defines personal data as various information relating to an identified or identifiable natural person recorded by electronic or other means.

While most laws and regulations do not distinguish between electronic and non-electronic data, certain regulations (such as the CSL and the Regulations on Network Data Security Management) regulate only "network data", which refers to electronic data processed and generated through networks, and are therefore electronic by nature.

3.1.4. Other key definitions pertaining to data and its processing

(1) "Processing": According to the PIPL, the processing of personal data includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion etc. of personal information/data.

(2) "Personal Data Processor": Different from the GDPR, the PIPL does not use the term "controller" to refer to entities that hold or process personal data. Instead, it names such entities as "Personal Data Processor". According to the PIPL, a Personal Data Processor is defined as an organization or individual that independently determines the purpose and method of the processing of personal data.

(3) "Entrusted processing party": Instead of using the term "processor" in GDPR, the PIPL sets out the scenario of entrusted processing of personal data. An "Entrusted processing party" refers to an individual or an organization being engaged or entrusted by others to process personal data in accordance with its instructions and is akin to the concept of "processor".

(4) "Data Subject": The PIPL does not define "data subject". As both the Civil Code and the PIPL provide that a natural person's personal data shall be protected by law, it is generally understood that a natural person/individual identified by the personal data shall be regarded as a data subject.

(5) "De-identification": According to the PIPL, it refers to the process in which personal data is processed so that it is impossible to identify certain natural persons without the aid of additional information.

(6) "Anonymization": According to the PIPL, it refers to the process through which personal data is irreversibly processed using technical means to ensure that specific individuals cannot be identified, and the original data cannot be restored.

3.2. Statutory exemptions

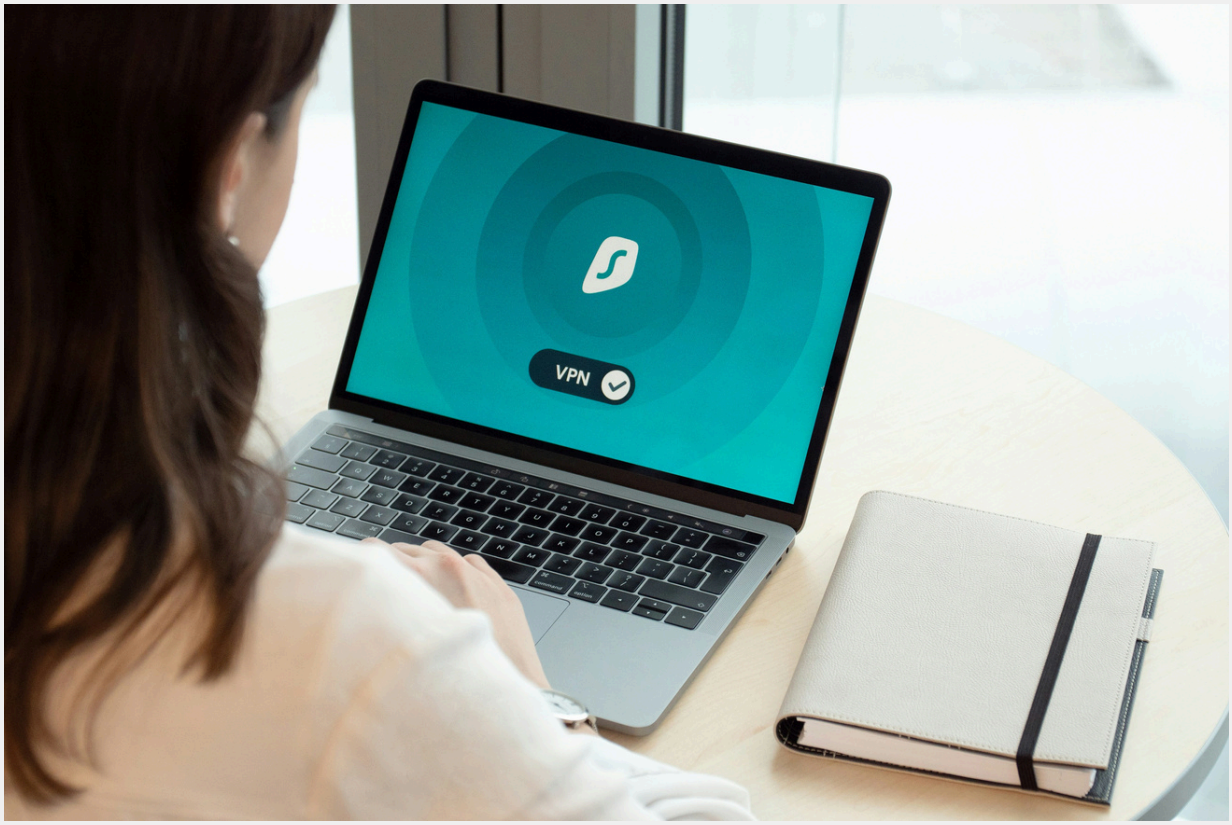
China has provided several statutory exemptions for regulations of personal data, including:

(1) According to Article 4 of the PIPL, the law only regulates personal data, excluding information that has been anonymized.

(2) According to Article 72 of the PIPL, the law doesn't apply to the processing of personal data by a natural person for personal or family affairs. Besides, where laws or administrative regulations provide for the processing of personal data in statistical and archival management activities organized and implemented by China's governments at all levels and their relevant departments, such provisions shall apply.

3.3. Territorial and extra-territorial application

The PIPL applies to the processing of personal data of natural persons within the territory of China. For extra-territorial application, according to Article 3 of the PIPL, the law also applies to the processing of personal data of natural persons within the territory of China that is



carried out outside the territory of China under any of the following circumstances:
(1)For the purpose of providing products or services to natural persons within China;
(2)To analyze or evaluate the behavior of natural persons within China;
(3)Other circumstances as stipulated by laws and administrative regulations.

Legislative Framework

4.1. Key stakeholders

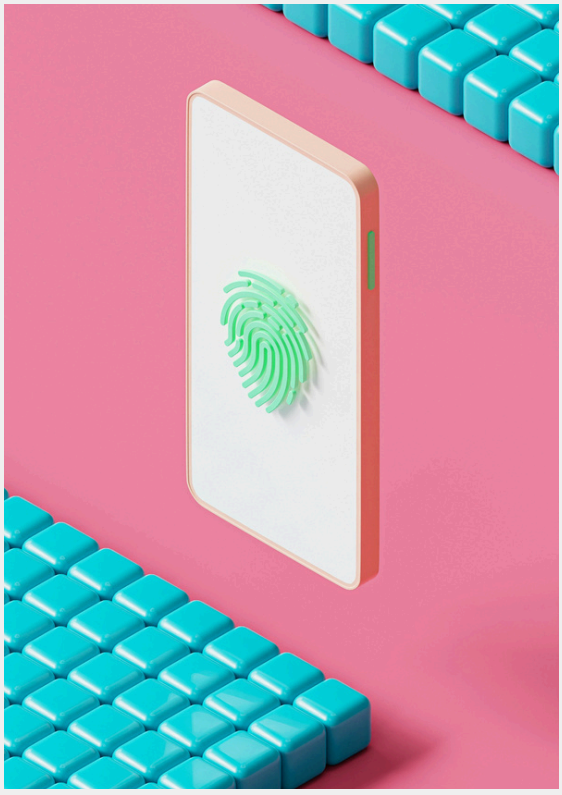
(1) Personal Data Processor: According to the PIPL, it refers to an organization or individual that can make its own decision on the purpose, the means of processing, and other matters relating to the processing of personal data. A Personal Data Processor acts as the key stakeholder of personal data protection obligations and liabilities under the PIPL, and is similar to the concept of "controller" under the GDPR (while the concept of "entrusted processing party", i.e., an individual or an organization being engaged or entrusted by other(s) to process personal data in accordance with its instructions, is similar to the concept "processor" under the GDPR).

(2) Individual: An individual act as the personal data subject under the PIPL, and is entitled to a series of rights.

(3) Personal information protection officer (PIPO): According to the PIPL and the national CAC's Announcement on Submitting Personal Information Protection Officer Information, Personal Data Processors that process personal data of over 1 million individuals shall designate a PIPO.

4.2. Role and responsibilities of key stakeholders

(1) Personal Data Processor: Under the PIPL, a Personal Data Processor shall follow requirements throughout the processing procedure of personal data, i.e., the collection, storage, use, processing,



transmission, provision, disclosure, and deletion, etc. For a detailed description, please refer to the following section, "6. Requirements for Data Processing".

(2) Individual: Under the PIPL, an individual is entitled to a series of personal data subject rights. For a detailed description, please refer to the following section "6. Rights and duties of data providers/principals".

(3) Personal information protection officer (PIPO): A PIPO shall be responsible for supervising personal data processing activities and the protective measures taken. Meanwhile, a Personal Data Processor shall disclose a PIPO's contact information and report a PIPO's name and contact details to the municipal-level CAC in the city where it is located.

Requirements for Data Processing

5.1. Grounds for collection and processing

5.1.1. Consent

Generally, personal data may only be collected and processed with the data subject's informed, freely given, and explicit consent.

In certain circumstances, separate consent is required. For instance, when processing sensitive personal data, sharing personal data with third parties, or transferring personal data across borders. Unlike "general consent", which covers multiple purposes with a single approval, separate consent requires clear and specific authorization for each individual processing activity.

Nevertheless, the PIPL allows for limited exceptions where personal data may be processed without consent, such as when processing is necessary for the performance of a contract to which the data subject is a party, or when it is carried out for lawful HR management. Despite these exceptions, consent remains the primary legal basis for the collection and processing of personal data under PIPL.

5.1.2. Consent notice

In addition to obtaining consent, a Personal Data Processor must provide a clear, comprehensive, and accessible privacy notice or policy. This notice must clearly explain how personal data is collected, processed, shared, and stored, specifying the purposes, scope, methods, and retention periods of each processing activity. It must also outline the full range of data subject rights, along with the procedures and methods to exercise those rights in practice.

To ensure clarity and accessibility, the privacy notice should be written in concise and unambiguous language that is easy to understand. It must be made available to the data subject at the time consent is collected and remain continuously accessible. Furthermore, the notice should be promptly updated to reflect any material changes to the Personal Data Processor's data processing practices, and additional consent should be sought if such changes affect the original scope or purpose of processing.

5.1.3. Withdrawal of consent

Where the processing of personal data is based on the data subject's consent, the data subject has the right to withdraw such consent at any time. The Personal Data Processor must provide a convenient and accessible method for the data subject to exercise this right. Upon withdrawal of consent, the Processor must delete the relevant personal data, either proactively or upon the data subject's request.

5.2. Data storage and retention timelines

Unless otherwise required by applicable laws or administrative regulations, personal data should only be retained for the minimum period necessary to fulfill the purpose for which it was collected. Once that purpose has been achieved, or the agreed retention period has expired, the personal data must be deleted.

Exceptions are where laws and regulations provide for a minimum retention period for certain types of personal data; such requirements shall be followed.

5.3. Data correction, completion, update, or erasure

Data subjects have the right to ensure their personal data is accurate, complete, and up-to-date. Personal Data Processors are legally required to address such requests promptly, reasonably, and effectively. For instance, upon receiving a valid request for data deletion, the Personal Data Processor must promptly erase the relevant personal data, unless retention is necessary to fulfill legal obligations. A detailed outline of the rights of data subjects is provided in section "6. Rights and Duties of Data Providers/Principals."

5.4. Data protection and security practices and procedures

5.4.1. Organizational measures

(1) Internal management systems and operational procedures

Personal Data Processors must implement clear internal policies and procedures that outline processing workflows and authorization protocols. High-risk operations—including bulk data deletion, copying, or downloading—require formal approval. All unauthorized activities must be logged and reviewed.

(2) Data categorization and risk-based management

Personal data shall be classified based on sensitivity levels and potential impact severity, with differential safeguards implemented according to each classification tier.

(3) Personnel training

All staff with access to personal data must complete role-specific security training at least annually. The training program should cover both general data protection principles and job-specific responsibilities.

(4) Security incident response plan

Personal Data Processors should establish and maintain an emergency response plan for personal data security incidents. The plan should define clear procedures for detecting, logging, assessing, containing, notifying, and reporting incidents. Annual drills are required to ensure the effectiveness of the plan.

5.4.2. Technical measures

Referencing the "Guidelines for Personal Information Security Protection on the Internet", organizations must implement technical safeguards across the entire data lifecycle—collection, storage, transmission, usage, and deletion. Key requirements include:

- **Data Encryption:** Use secure protocols such as SSL/TLS (e.g., HTTPS) for data transmission, and store sensitive personal data using robust encryption algorithms such as AES, ensuring that leaked data cannot be read in plaintext.

- **Data Desensitization and Anonymization:** Apply masking or replacement for sensitive data. Techniques such as k-anonymity or differential privacy should be used to prevent data from being traced back to identifiable individuals.

- **Access Control and Access Management:** Enforce minimum necessary access authorization. Strengthen authentication using passwords, SMS verification codes, or biometric methods.

- **Data Backup and Disaster Recovery:** Implement the 3-2-1 backup strategy—maintain at least three copies of data, stored on two different media, with one copy offsite. Conduct regular drills to test recovery procedures.

- **Data Loss Prevention (DLP) and Log Auditing:** Monitor and block unauthorized transmission of sensitive data. Maintain comprehensive audit logs of access, modification, and deletion activities.

- **Secure Development and Configuration Management:** Implement source code obfuscation and hardening techniques. Ensure database access rights are properly separated and managed.

5.5. Disclosure, sharing, and transfer of data

If a Personal Data Processor intends to share, disclose, or transfer an individual's personal data to a third party (including its affiliated companies), the Processor must:

- Inform the data subject in advance about the purpose of the transfer, the types of personal data involved, and the recipient's name and contact details, and obtain the data subject's explicit prior consent when the third party acts as a separate Personal Data Processor;

- Conduct a personal data impact assessment (PIA) to evaluate risks associated with the transfer, and implement appropriate safeguards—such as data transfer agreements or equivalent contracts—based on the assessment results to protect the data subjects;

- Keep accurate records of the sharing, disclosure, or transfer, including the date, scope, purpose, and basic information of the recipient;

- Transfer personal data only when necessary for processing purposes, and avoid sharing or transferring personal biometric data or other particularly sensitive information if prohibited by relevant laws or regulations; and

- Establish contractual terms that require entrusted data processors to comply with data protection obligations or assist the Personal Data Processor in fulfilling these obligations.

5.6. Cross-border transfer of data

5.6.1. Legitimate mechanisms

Before transferring personal data overseas, Personal Data Processors must implement one of the three lawful mechanisms provided by the PIPL—unless an exemption applies.

(1)CAC Security Assessment

A Personal Data Processor must undergo a security assessment conducted by the CAC if it transfers important data overseas, is classified as a Critical Information Infrastructure Operator (CIIO), or has processed personal data above certain thresholds (where an entity exports personal information of more than one million people, or sensitive personal information of more than ten thousand people since January 1 of a given year).

Before submission, the Processor must complete a self-assessment to evaluate risks posed by data transfer to national security, public interest, and individual rights. The report is submitted to both provincial and national CAC offices.

If approved, the CAC will issue a decision valid for three years, renewable for another three if no major changes occur in the transfer.

(2) Standard Contractual Clauses (SCCs)

If the Personal Data Processor does not meet the CAC's security assessment thresholds, it may adopt the Standard Contractual Clauses (SCCs) mechanism. This applies to cross-border transfers involving personal data within certain thresholds (where an entity exports personal information of over 100,000 people, or any sensitive personal information, since January 1 of a given year).

Under this approach, the Processor must sign an SCC with the overseas recipient and, within 10 working days

of its effective date, submit the signed contract and a corresponding PIA to the local CAC office.

(3) Certification

The certification mechanism applies to Personal Data Processors that meet the same thresholds as those under the SCC mechanism. Notably, this route offers a more practical and accessible option for overseas entities without a presence in China, which have faced challenges in complying with other cross-border transfer mechanisms under the PIPL.

5.6.2. Exempted transfers

Despite the three mechanisms outlined above, certain cross-border data transfers are exempt from these requirements. For instance, transfers conducted under international treaties to which China is a party, or those necessary for fulfilling contracts involving individuals, as well as lawful cross-border human resources management, may be exempt.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

6.1.1. Right to be informed, right to make decisions, and right to restrict or refuse processing

Data subjects have the right to be informed about the processing of their personal data and to make decisions regarding such processing. They also have the right to restrict or refuse the processing of their personal data by others.

6.1.2. Right to access and copy

Data subjects have the right to request access to and obtain copies of their personal data from the data processor.

6.1.3. Right to data portability

Where technically feasible and in accordance with conditions prescribed by the CAC, data subjects have the right to request the transfer of their personal data to a designated data processor. The original data processor must provide the means for such transfer where the legal requirements are met.

6.1.4. Right to rectification and supplementation

If a data subject discovers that their personal data is inaccurate or incomplete, they have the right to request correction or supplementation. The processor must make the necessary changes in a timely manner upon verification.

6.1.5. Right to deletion

Data subjects have the right to request the deletion of their personal data under circumstances prescribed by law, such as where the processing purpose has been fulfilled, consent has been withdrawn, or the data has been unlawfully processed.

6.1.6. Right to explanation

Data subjects have the right to request that the data processor explain its rules for processing personal data, including the purposes, methods, categories of data involved, and data retention policies.

6.1.7. Rights of close relatives of deceased individuals

*I*n the event of the death of a natural person, close relatives of the deceased may, for their own lawful and legitimate interests, exercise rights to access, copy, correct, or delete the deceased's personal data, unless the deceased had made other arrangements prior to death.

Processing of the data of Children or Minors

Under the PIPL, personal data of children under the age of 14 shall be regarded as sensitive personal data, the processing of which shall be subject to additional legal requirements. Personal Data Processors are obligated to implement specific measures to ensure the security and appropriateness of such data processing, including:

- *Parental or Guardian Consent*: *data collection and processing must be authorized by the parent or guardian through a clear and informed consent process tailored to minors.*
- Specialized Processing Policies: Personal Data Processors must establish specific policies for children's data, including privacy notices designed for both minors and their guardians, data minimization practices, and robust security measures to safeguard the information.
- Access and Erasure Rights: Parents or guardians retain the right to access, correct, or request the deletion of their child's personal data at any time.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

In China, there is no single authority solely responsible for enforcing personal data protection laws. Instead, a range of law enforcement departments share regulatory responsibilities. Among all these regulators, the most important ones include:

- The Cyberspace Administration of China (CAC).
- The Ministry of Public Security (MPS).
- The Ministry of Industry and Information Technology (MIIT).

In practice, regulatory authorities such as the People's Bank of China (PBOC), State Administration for Market Regulation (SAMR), and the China Securities Regulatory Commission (CSRC) also exercise oversight over data processing activities within their respective jurisdictions.

8.2 Roles, functions, and powers of authorities

8.2.1. CAC

The CAC leads overall coordination of personal data protection, formulates policies, issues guidelines, enforces compliance, conducts inspections, and oversees cross-border data transfer security assessments. It has broad enforcement powers, including investigations, ordering corrective actions, imposing penalties, and maintaining blacklists.

8.1.2. MPS

The MPS focuses on cybersecurity and public safety, investigating and punishing data-related crimes such as data theft and unauthorized data trading. It supervises critical information infrastructure and national security, conducting criminal investigations and coordinating joint regulatory actions.

8.2.3. MIIT

The MIIT regulates telecommunications and internet sectors, ensuring lawful personal data handling by network operators and digital service providers. It issues industry regulations, conducts inspections, orders rectifications, and enforces penalties related to data protection.

8.2.4. SAMR

The State Administration for Market Regulation (SAMR) is responsible for personal information protection in the areas of consumer rights and market order. Under laws such as the CSL, E-commerce Law, and Consumer Protection Law, market regulators are authorized to investigate and address personal data violations. SAMR primarily carries out enforcement through its affiliated bodies, such as the China Cybersecurity Review Technology and Certification Center (CCRC).

8.3. Roles, function,s and powers of civil/criminal courts in the field of data regulation

8.3.1. Civil Courts

Civil courts handle disputes over personal data misuse, enforcing rights under the PIPL and Civil Code. They can order compensation, injunctions against unlawful processing, and hear public interest litigation.

8.3.2. Criminal Courts

Criminal courts prosecute offenses such as illegal buying or selling of personal data, cybercrimes, and serious violations of data rights. Penalties include imprisonment, fines, and confiscation of illegal gains.

Consequences of non-compliance

9.1. Consequences and penalties for data breach

Under the PIPL, data breaches—including unauthorized access, leakage, tampering, or loss due to inadequate protection—require prompt remedial action and notification to affected individuals and regulators such as the CAC. Non-compliance can result in administrative penalties like warnings, orders to rectify violations, suspension of data processing activities, or even revocation of business licenses. Severe breaches may incur fines up to RMB 50 million or 5% of annual revenue.

9.2. Consequences and penalties for other violations and non-compliance

The PIPL also penalizes unlawful data collection, lack of valid consent, unauthorized cross-border transfers, and failure to conduct required security assessments. Violations may lead to fines, suspension of data processing, blacklisting, and heightened regulatory scrutiny. In addition to penalties on the organization, responsible individuals—such as executives or data protection officers—may face personal fines or be restricted from holding management roles. Authorities may also increase oversight through on-site inspections and mandatory compliance audits.

Conclusion

China's data privacy protection regime is built on the Three Fundamental Laws, with the PIPL acting as the cornerstone. The PIPL requires the processing of personal data to be lawful, legitimate, and necessary, and despite many exemptions provided for in the law, informed consent remains the most-relied-upon legal ground to process personal data for Personal Data Processors in China. In addition to the PIPL, many other laws and regulations govern the processing of personal data in specific industries (such as healthcare and automobile) or using specific means (such as AI). Moreover, data compliance under Chinese law also requires reference and conformity to non-binding national standards, as they may be used by law enforcement authorities to interpret laws and regulations.

Contact Us

+86 21 3135 8701

www.llinkslaw.com

david.pan@llinkslaw.com

19F, ONE LUJIAZUI, 68 Yin Cheng Road Middle, Shanghai 200120 P.R.China

Czech Republic

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) is the EU regulation that is directly applicable in all member states of the EU, including the Czech Republic, as of 25 May 2018. The new Czech Act No. 110/2019 Coll., on Processing of Personal Data, which partly implements the GDPR in the Czech Republic, is effective as of 24 April 2019. The Act on Processing of Personal Data replaced the previous Act No. 101/2000 Coll., on Protection of Personal Data, as amended. Among other things, this new act regulates the jurisdiction of the Office for Personal Data Protection as the main data protection authority in the Czech Republic. The other laws briefly described below contain special rules for specific areas that apply together with or beside the general rules on personal data protection and processing.

Contact Us

+420 246 085 300

www.peterkapartners.com/

hradil@peterkapartners.cz

Karlovo náměstí 671/24
110 00 Praha 1

Governing Data Protection Legislation

2.1 Overview of principal legislation

- the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR");
- the Act no. 110/2019 Coll., on the Processing of Personal Data, as amended (this act implements the GDPR in the Czech Republic).

2.2 Additional or ancillary regulation, directives, or norms

- the Act No. 89/2012 Coll., Civil Code, as amended (with general rules on privacy in section 84 and following);
- the Act No. 262/2006 Coll., Labour Code, as amended (it stipulates some rules on privacy in employment, namely in section 316 of the Labour Code);

- the Act No. 480/2004 Coll., on Certain Information Society Services and on Amendments to Certain Acts, as amended ("**Act on Certain Information Society Services**") (the dissemination of commercial communications by electronic means, such as by e-mail or telephone, is regulated by this act). This act implements the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") and the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ("**ePrivacy Directive**" or "**ePD**");

- the Act No. 127/2005 Coll., on Electronic Communications and on Amendment to Certain Related Acts (**Act on Electronic Communications**), as amended (this act regulates the marketing phone calls, use of cookies, and processing of personal data in telecommunications). This act implements, among others, the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, and also the ePrivacy Directive/ePD;

- the Act No. 264/2025 Coll., on Cyber Security, as amended (with several obligations, for example, the registration obligation and the obligation to report security incidents under the Cyber Security Act, in addition to the obligation to report data breaches under the GDPR/eDP – in case the data breach involves also security incident).

2.3 Upcoming or proposed legislation (if applicable)

- the new Act on Cyber Security, effective as of 1 November 2025, mentioned above, will replace the previous cybersecurity act in the Czech Republic. This new act is implementing the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Scope of Application

3.1. Legislative Scope

The general rules for the protection and processing of personal data in the Czech Republic are stipulated in Act No. 110/2019 Coll., on the Processing of Personal Data, as amended ("Act on Processing of Personal Data"), and Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons about the processing of personal data and on the free movement of such data, and

repealing Directive 95/46/EC – (General Data Protection Regulation) ("GDPR").

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – (General Data Protection Regulation) ("GDPR").

3.1.1. Definition of personal data

The same as in the GDPR.

3.1.2. Definition of different categories of personal data

There are no special definitions of other personal data, except for the regulation of birth number, which is a unique identifier (identification number) of natural persons in the Czech Republic (similar to a social security number in other countries).

There are other terms, such as "sensitive data" or "sensitive personal data, " used in previous law and legal regulations (where these previous laws and/or regulations use the terms above, this basically means special categories of personal data under the GDPR – see also point 3.2 below).

3.1.3. Treatment of data and its different categories

- **Regulation of personal and non-personal data**

The personal data and their processing are regulated, namely, by the GDPR and the Act on Processing of Personal Data. As for non-personal data, the safety of selected networks

and provision of relevant services by selected obliged persons is regulated, namely, by the Cyber Security Act.

- **Regulation of electronic and non-electronic data**

There is no special regulation distinguishing the data based on the form of data (electronic or non-electronic), the regulation of personal data applies to all data disregarding their form, with very few exceptions (such as special regulation for direct marketing via e-mail or phone calls, which is regulated mainly by the Act on Certain Information Society Services and the Act on Electronic Communications).

3.1.4 Other key definitions pertaining to data and its processing

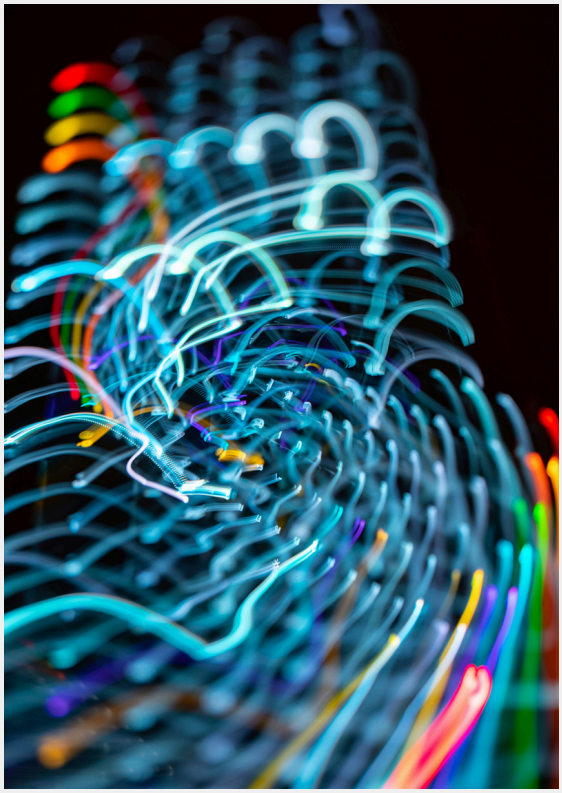
The definitions are the same as in the GDPR; the Act on Personal Data Processing does not contain any different or special definitions related to personal data and its processing.

3.2. Statutory exemptions

There are only a few exemptions or special requirements under the Czech law in addition to the GDPR. The most important ones are briefly described below:

- The implementation of Article 6.2 of GDPR: Article 6.2 of GDPR has only been partially addressed in the Act on Processing of Personal Data, namely in Title II, Personal Data Processing Pursuant to Directly Applicable Regulation of the European Union (i.e., GDPR), Chapter 1 (namely sections 5, 6, 8, 9, 10, 11, 12, and 14). Chapter 2 deals with Personal Data Processing for Journalistic Purposes or Purposes of Academic, Artistic, or Literary Expression.

- The implementation of Article 8.1. of GDPR: Under section 7 of the Act on Personal Data Processing, there is a fifteen-year-old limit for a child to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child (for more details see point 7 below).



Czech Republic

- The implementation of Article 9.4 of GDPR: Article 9.4 of GDPR has not been expressly addressed in the Act on Processing of Personal Data implementing the GDPR in the Czech Republic, it only mentions these data (genetic, biometric data or of data concerning health) in section 66 (Transitory Provisions), together with other data referred to as "sensitive data" or „sensitive personal data" in previous law and legal regulations (where these previous laws and/or regulation use the terms above, this basically means special categories of personal data under the GDPR).

- The implementation of Article 23.1 of GDPR: Article 23.1 of GDPR has been addressed in the Act on Processing of Personal Data implementing the GDPR in the Czech Republic, namely in Title II, Personal Data Processing Pursuant to Directly Applicable Regulation of the European Union, and Title IV, Personal Data Protection in Ensuring Defence and Security Interests of the Czech Republic.

- The implementation of Article 35.4 of GDPR: In the implementation of Article 35.4 of GDPR, the Office has issued the lists and the methodologies related to DPIA (the Office published not only the list of activities under Article 35(4) of the GDPR, but also the list of activities under Article 35(5) of the GDPR).

- The implementation of Article 35.10 of GDPR: Under section 10 of the Act on Personal Data Processing, the controller does not have to assess the impact of the processing on the protection of personal data (DPIA) before it begins, if the legal regulation requires them to carry out such processing of personal data.

- The implementation of Article 87 of GDPR: The regulation of the use of the birth (identification) number is contained in the Act No. 133/2000 Coll., on the Registration of Population and Birth Numbers and on the Amendment of Certain Acts (the Act on Population Registration). Pursuant to Section 13(9) of this act, only the natural person to whom the birth number has been assigned (or his / her legal representative) is entitled to use it or decide on its use within the limits stipulated by law; otherwise, the birth number may be used only in the cases specified in Section 13c of this act.

- The implementation of Article 88 of GDPR: The implementation of Article 88 of GDPR, which deals with processing in the context of employment, has been dealt with, namely, in section 316 of the Labour Code.

3.3 Territorial and extra-territorial application

In general, the laws of the Czech Republic apply within the territory of the Czech Republic. As for the GDPR, the provisions of Article 3 apply, including extraterritorial application of the GDPR.

Legislative Framework

4.1 Key stakeholders

- There are no derivations based on the local law from the definitions in the GDPR, i.e., the definition for each stakeholder, such as 'Data Controller', 'Data Processor', 'Data Subject,' etc., are the same as under the GDPR.

4.2 Role and responsibilities of key stakeholders

All key stakeholders must be able to prove that they fulfil all requirements stipulated by personal data protection laws, including the Czech local law and the GDPR. As for the language, the Office may require Czech translations or Czech versions of the Czech companies (as data controllers or data processors) documents on personal data processing/protection. Under the Czech law, there is no express provision regarding the language in which such internal guidelines/policies/documentation should be drafted. However, in the field of data protection, the activity carried out by a controller/processor is subject to investigation by the Czech authorities, namely the Office, based on the Czech law. In this respect, the Czech authorities may require either bilingual documents or certified translations into Czech language of documents issued in a different language. Thus, at least a bilingual version, including Czech version or a certified translation into Czech should be available for the relevant authorities.

Requirements for Data Processing

5.1 Grounds for collection and processing

- Consent: No derivations from the GDPR.
- Consent Notice: No derivations from the GDPR.
- Withdrawal of Consent: No derivations from the GDPR.

5.2 Data storage and retention timelines

There are no explicit general rules stipulating data retention periods; only some special laws mention such periods. For example, personal data that need to be processed for accounting purposes must be, generally, kept for 5 years as of the end of accounting period for all accounting documents if not stipulated otherwise (under the Accounting Act), 10 years for financial statements and annual reports (under the Accounting Act), for VAT purposes under the Value Added Tax Act) and for social security payments purposes (under the Act on Social Security Contributions and Contribution to the State Employment Policy)

Tor generally for tax purposes (under the Act on Income Taxes and the Tax Code) and 45 years for pension purposes must be kept up to (under the Act on the Organization and Implementation of Social Security). If the personal data are needed for debt collection, they must be kept until the end of the first financial year following the financial year in which the debt was paid or obligation met (under the Accounting Act).

Where accounting units use accounting records not only for the purpose pursuant to the Accounting Act, but also for other purposes, in particular for purposes relating to criminal proceedings, measures against money-laundering (keeping the records for 10 years), administrative proceedings, civil judicial proceedings, tax proceedings or special proceedings concerning the destruction of certain documents, or for the purposes of social security, general health insurance or copyright protection, after expiry of the storing periods above, the accounting units are obliged so proceed as to ensure compliance with the requirements ensuing from the use of accounting records for such other purposes; in cases in which the accounting units use their accounting records for such purposes, all the provisions of the Accounting Act similarly apply.

As for the CCTV recordings, based on the opinions of the Office, the standard retention period recordings from CCTV, is 3 to 7 days in the Czech Republic. Any longer retention period must be justified by the circumstances of the particular case (unless there are special rules stating otherwise, such as regulations for gambling).

As for the traffic and location data, the data retention is regulated in the Czech Republic by the Act on Electronic Communications. Under Sec. 97(3) of the Act on Electronic Communications, a legal entity providing a public communications network or a publicly available electronic communications service is obliged to store traffic and location data for a period of 6 months and is obliged to disclose such data (including metadata) to the relevant authorities (e.g., police) on request (please note that this applies only to providers of services under the Act on Electronic Communications).

5.3. Data correction, completion, updation, or erasure of data

No derivations from the GDPR.

5.4. Data protection and security practices and procedures

No derivations from the GDPR. The Office publishes guidelines of the EDPB and also its own guidelines regarding selected security practices and procedures in the personal data protection area.

5.5. Disclosure, sharing, and transfer of data

No derivations from the GDPR.

5.6. Cross-border transfer of data

No derivations from the GDPR.

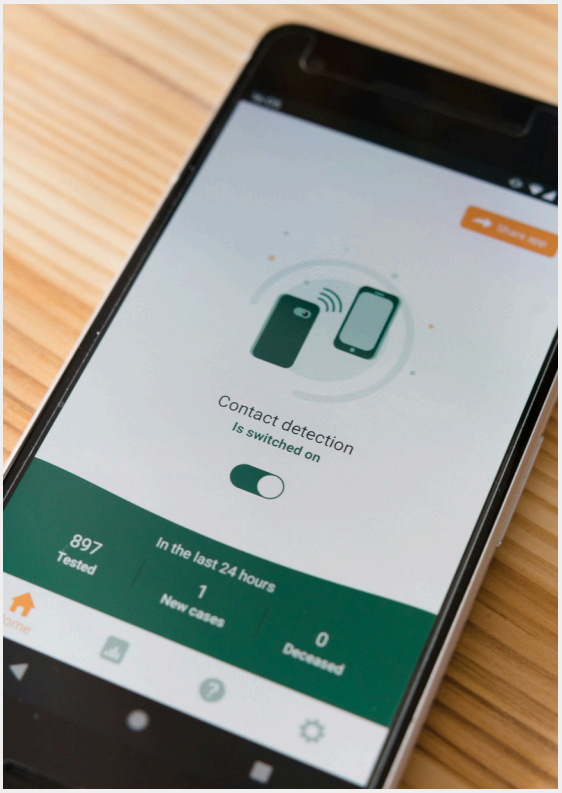
5.7. Grievance redressal

No derivations from the GDPR. In most cases, the Czech Office for Personal Data Protection is the local DPA (data protection authority) who deals with complaints.

Rights and Duties of Data Providers/Principals

6.1 Rights and remedies

- Right to withdraw consent: No derivations from the GDPR, if the processing is based on consent, the consent may be withdrawn anytime.



- Right to grievance redressal and appeal: The Czech Office for Personal Data Protection (Office) is the local DPA (data protection authority) that deals with complaints. It is possible to file an appeal against the decision of the Office to the Chairperson of the Office. It is possible to file an administrative action in the Municipal Court in Prague against the final decision of the Office.

- Right to access information: No derivations from the GDPR.

- Right to nominate: There is no explicit regulation of the right to nominate in the Czech law regardingthe processing of personal data. Primarily, it is the data controller who is responsible for data processing activities and performing related duties. Personal data controller may appoint personal data processor(s) to perform some of these data processing activities.

6.2 Duties

As for the data processing, the duties of data controllers and data processors are the same as under the GDPR. For the main roles and responsibilities of key stakeholders, including language requirements, please see the above point 4.2. For the main

Processing of Children or Minors' data

As regards the consent of minors for the data processing, referred to in Article 8.1 of GDPR, this provision has been implemented by section 7 of the Act on Personal Data Processing (Capacity of Child to Grant Consent to Personal Data Processing), under which *"A child shall enjoy capacity to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child from fifteen years of age".*

Regulatory Authorities

8.1 Overview of relevant statutory authorities

- The Czech Office for Personal Data Protection (ÚOOÚ)
- The Czech Telecommunication Office (ČTÚ)
- The National Cyber and Information Security Agency (NÚKIB) and CZ.NIC

8.2 Role, functions, and powers of authorities

- Role functions and powers of principal data regulation authority (if applicable): In the Czech Republic, the Office for Personal Data Protection (hereinafter "Office") supervises observance of the legal obligations laid down for the processing of personal data as the main authority in this area. Supervision in the form of inspection

is performed pursuant to a special act (Act no. 255/2012 Coll., on Inspection (Inspection Code), as amended). The Office does not deal with disputes between the controllers or the processors and data subjects or other natural or legal persons/entities arising from contractual or pre-contractual relations.

The Office is also responsible for dealing with data subjects' complaints on unsolicited commercial messages under the Act on Certain Information Society Services (i.e., it receives and solves these complaints).

- Role, functions, and powers of additional or ancillary data regulation authorities (if applicable): In the Czech Republic, the National Cyber and Information Security Agency (NÚKIB) supervises observance of the legal obligations laid down for the obliged persons by the Cyber Security Act. The Czech Telecommunication Office is responsible for dealing with data subjects' complaints against unsolicited marketing phone calls under the Act on Electronic Communications (i.e., it receives and solves these complaints).

8.3 Role, function,s and powers of civil/criminal courts in the field of data regulation

The Czech civil courts deal with disputes between the controllers or the processors and data subjects or other natural or legal persons/entities arising from contractual or pre-contractual relations and also from the liability relations (damages).

The Czech administrative courts decide on administrative actions filed against decisions of the Czech administrative bodies/authorities, including the Office as mentioned in point 6.1 above.

The Czech criminal courts deal with crimes committed in the field of data protection, such as Unauthorised Use of Personal Data under section 180(2), Unauthorised Access to Computer Systems and Information Media under section 230(2) or Violation of Copyright, Rights Related to Copyright and Database Rights under section 270 of the Czech Penal Code (the Act no. 40/2009 Coll.).

Consequences of non-compliance

9.1 Consequences and penalties for data breach

Infringements of the GDPR are subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

9.2 Consequences and penalties for other violations and non-compliance

If the Office finds that obligations imposed by the law have been breached, the Office will determine which measures must be adopted to eliminate the established shortcomings and set a deadline

for their elimination. If the shortcomings are eliminated in accordance with the determined measures or immediately after the breach of obligation is found, the Office may decide not to impose fines. If the fines are imposed, the general rules of the GDPR apply. Infringements of the GDPR are subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In case of commercial messages, legal entities may be fined up to CZK 10,000,000 (approximately EUR 405,000) for disseminating commercial communications in violation of the Certain Information Society Services Act. The Czech Office for Personal Data Protection (Office) is the authority for supervision of compliance with this act. In addition, fines and other measures may apply under the GDPR in case of breach of rules for processing of personal data (please see above).

Unsolicited/harassing phone calls (i.e., also marketing phone calls without consent unless the exception applies) are considered misdemeanours under the Act on Electronic Communications. The Czech Telecommunication Office supervises compliance with the Czech Act on Electronic Communications, and has the authority to issue binding decisions, including prohibitions or orders and fines for violations. Legal entities may be fined up to CZK 50,000,000 (approximately EUR 2,022,000) or 10 % of the total worldwide annual turnover of the preceding financial year for unsolicited/harassing phone calls in violation of the Act on Electronic Communications.

Conclusion

The Czech Republic has implemented the GDPR mainly through the Act on Processing of Personal Data, as mentioned above. There are also other laws that deal with the same or similar issues as the GDPR, but the GDPR remains the main law in the area of data protection, and there are only very few additional requirements and derivations from the GDPR in the Czech Republic.

As for the new legislation, the new Act on Cyber Security (effective as of 1 November 2025 in the Czech Republic) implementing the NIS 2 Directive will substantially broaden the number of entities to which this new Czech law will apply (from approx. 400 entities under the previous law to approx. 6,000 entities under the new law).

Germany

Germany maintains a high level of data protection, closely integrated into the European legal framework. The EU General Data Protection Regulation (GDPR), effective since 25 May 2018, provides the primary framework. In parallel, the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) was enacted on the same day, implementing national provisions and filling GDPR's opening clauses. The German Constitutional Court (Bundesverfassungsgericht) has recognized a fundamental right to informational self-determination since 1983, emphasizing the constitutional weight of privacy. Overall, the German data protection regime is shaped by the GDPR as the common European framework, supplemented by the BDSG and further sector-specific regulations.

Core Data Protection Laws and Regulations

GDPR and BDSG: As an EU regulation, the GDPR applies directly in Germany. The BDSG 2018 adds national rules, notably in the fields of employment data, processing of special categories of personal data (such as health data for social purposes), and certain derogations for scientific research, statistics, and archiving. Part 3 of the BDSG transposes Directive (EU) 2016/680 (Law Enforcement Directive). In addition, Germany has numerous sector-specific data protection laws (e.g., in finance, energy) which must be applied consistently with the GDPR.

Supervisory authorities: Unlike some EU Member States, Germany does not have a single central supervisory authority. Instead, each federal state (Bundesland) has its own Data Protection Authority, and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) oversees federal authorities and specific sectors. These regulators coordinate within the Conference of the Independent Data Protection Supervisory Authorities (Datenschutzkonferenz; DSK) to ensure harmonized enforcement across Germany.

Mandatory Data Protection Officers (DPOs): Germany has extended the GDPR's requirement under Article 37. Pursuant to § 38 BDSG, a company must appoint a DPO if at least 20

Contact Us

+49 - 69 - 4500 13 525

https://www.omf-law.com

jan.koenig@omf-law.com

MesseTurm | Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

employees regularly process personal data. Even below this threshold, a DPO is required if processing operations pose particular risks (e.g., processing subject to a Data Protection Impact Assessment or systematic processing for transfer/market research). This national rule is stricter than in most EU Member States. Regardless of the threshold, controllers remain obliged to implement appropriate security measures, conduct Data Protection Impact Assessments (DPIAs) where required, and notify data breaches to the competent authority within 72 hours.

Data Subject Rights: The GDPR's full catalogue of rights applies (access, rectification, erasure, restriction, portability, objection). The BDSG contains limited exceptions (e.g., §§ 34 - 35 BDSG allow restrictions to protect secrecy or public interests). German courts and regulators tend to interpret rights broadly in favor of data subjects. For example, in 2023, the Court of Justice of the EU (CJEU) clarified, on reference from German courts, that the right of access under Article 15 GDPR extends to internal access logs - i.e., information on when and for what purpose staff accessed personal data. This significantly increases the transparency obligations of controllers in Germany.

Recent National Developments

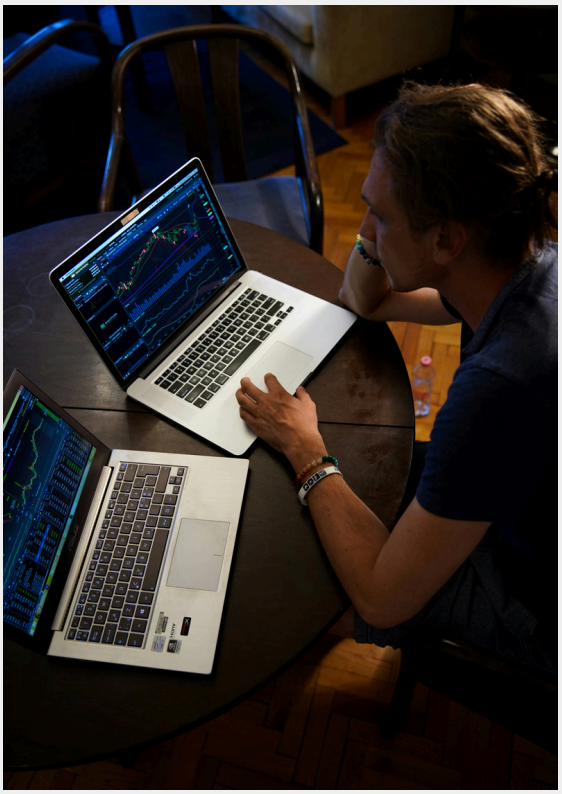
Employment Data Protection: Germany has long lacked a comprehensive statute on employee data, relying instead on § 26 BDSG. That provision broadly allows processing if necessary for hiring, carrying out, or terminating employment.

However, in March 2023, the CJEU ruled that a virtually identical state law (§ 23 HDSIG – Hesse Data Protection Act) was not a valid "specific measure" under Article 88 GDPR, as it merely repeated the Regulation's legal bases. In May 2023, the Federal Labor Court (BAG) held that § 26 BDSG is likewise incompatible with EU law and therefore inapplicable. Employers must thus rely directly on the GDPR legal bases (primarily Art. 6(1)(b) GDPR). In response, the Federal Government revived work on a dedicated Employment Data Protection Act. A draft framework (April 2023) and ministerial draft (October 2024) propose: clearer rules on monitoring in the workplace (open/secret), on the use of Artificial Intelligence in HR, an expanded scope (possibly covering platform workers), specific provisions for recruitment processes, rules on intra-group data transfers, and explicit conditions for voluntary employee consent. As of early 2025, no final law has been enacted, leaving employers in legal uncertainty.

Regulatory guidance: German regulators, via the DSK, regularly publish guidance papers. In May 2024, the DSK issued an extensive guidance paper on Artificial Intelligence and Data Protection, setting out criteria for GDPR-compliant AI deployment. It addresses issues such as lawful bases for training data, transparency obligations, and safeguarding rights against automated decisions.

Another hot topic is online tracking and advertising. In March 2023, the DSK issued a resolution on so-called "Pur subscription models" (pay-or-consent), stressing that consent must remain genuinely voluntary. In January 2024, the Cologne Higher Regional Court ruled that cookie banners must provide equally visible "accept" and "reject" options – a hidden or complicated "reject" button is unlawful.

Regulators also report growing complaint volumes, especially against Big Tech providers such as Meta and Google. German authorities have aligned their fine calculation method with the EDPB fining guidelines since 2023.



Case law: In December 2023, the CJEU's "Schufa" ruling declared that automated credit scoring is unlawful under Article 22 GDPR if it leads to adverse decisions without further human assessment. This has major implications for German credit bureaus and financial institutions. Earlier, in February 2023, the German Constitutional Court struck down provisions in Hesse and Hamburg authorizing automated data analysis by police using AI as unconstitutional, stressing the need for strict legal limits to protect the data of innocent individuals.

Adjacent Areas – Privacy & Security Outlook

IT Security (Cybersecurity)

Germany has a robust IT security regime under the Federal Office for Information Security Act (BSIG) and two IT Security Acts (2015 and 2021). Operators of critical infrastructure must meet minimum security standards and notify incidents. The NIS2 Directive (December 2022) significantly expands obligations (covering more sectors and more companies). Germany missed the October 2024 transposition deadline; a draft implementation law was only approved in July 2025, expected to apply to approximately 29,000 additional companies. In the meantime, existing BSIG rules apply. Cybersecurity is increasingly viewed as a core element of data protection compliance, as most data breaches result from insufficient security. The BSI's 2023 report highlighted ongoing threats, particularly ransomware and data theft.

E-Privacy and Telecommunications (TTDSG)

The Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG) entered into force on 1 December 2021, consolidating fragmented telecom/telemedia rules. In May 2024, it was renamed Telecommunications and Digital Services Data Protection Act (TDDG). Of particular relevance: § 25 TTDSG implements Article 5(3) ePrivacy Directive, requiring prior consent for cookies and tracking technologies - effectively Germany's statutory "cookie rule". The TTDSG also regulates the confidentiality of communications (calls, emails, messaging) and device data. Non-compliance can trigger fines in addition to GDPR penalties. The long-awaited EU ePrivacy Regulation is still under negotiation; until adopted, national rules remain binding. Recent German court rulings and DSK decisions confirm that manipulative "dark patterns" in cookie banners are unlawful.

Conclusion and Outlook

Germany's data protection regime is dense and mature, combining the GDPR with national rules and an active regulatory landscape. Key developments in 2023/24 included the invalidity of § 26 BDSG (employment data), the CJEU's Schufa ruling on credit scoring, and extensive supervisory guidance on AI and cookies.

Adjacent fields such as cybersecurity and ePrivacy continue to evolve – the delayed NIS2 implementation and the still-pending ePrivacy Regulation are central to watch. For 2025, employers should closely monitor the progress of the Employment Data Protection Act, while organizations more broadly must adapt compliance programs to new technologies (AI, tracking, cross-border data transfers). The German system is characterized by a strong privacy culture, proactive enforcement, and continuous legal developments. Businesses, law firms, and public bodies alike are well advised to regularly review policies, contracts, and security measures to meet Germany's stringent data protection standards.

Contact Us

+49 - 69 - 4500 13 525

https://www.omf-law.com

jan.koenig@omf-law.com

MesseTurm | Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

India

Introduction about the Firm

Ahlawat & Associates ("A&A") is one of the leading full-service law firms in India, catering both to domestic and international clients.

Incorporated in 1978 as primarily a litigation practice, A&A has steadily broadened its scope of expertise and services through the addition of new partners (in varied practice areas), emerging as one of the leading law firms in India. Our firm provides comprehensive counsel on various legal services such as mergers and acquisitions, private equity, real estate, education, intellectual property, media and entertainment, technology, online gaming, sports, data protection and privacy, virtual digital assets, employment, labor, licensing and registration, taxation (direct and indirect), and business setup (globally). With numerous attorneys in the firm possessing knowledge and experience across various fields of law, A&A is equipped to handle diverse legal requirements of our clients worldwide.

Our services extend through diverse sectors of industry to facilitate foreign direct investments and business setup in India. A&A has assisted and continues to assist clients from over 20 jurisdictions to enter and flourish in India by providing various legal options to best suit their needs. A&A takes pride in being amongst the most sought-after legal service providers globally.

A&A has been one of the leading law firms in the data protection and data privacy sector in India. It has assisted numerous domestic as well as international clients with various legal requirements in this specific legal domain, which includes assisting them with compliance under the relevant statutes, drafting of consent notices, preparation of internal data access control mechanisms, drafting of privacy policies, etc. A&A has also been extremely active in submitting inputs and comments to the Government on proposed legislation in this sector.

Contact Us

+91-11-41023400

www.ahlawatassociates.com

gaurav.bhalla@ahlawatassociates.in

Plot No. 66, LGF
#TheHub, Okhla Phase III, Okhla Industrial Estate
New Delhi, 110020 India

Introduction

The legal regime in India relating to data protection and privacy has undergone a significant overhaul and revamp. The Digital Data Protection Act, 2023 ("DPDPA") received the President's assent and was published in the official Gazette in India on August 11, 2023. Even though the DPDPA has been published in the Gazette, the date on which the statute will come into force is yet to be notified by the Government. The PDPA provides for the protection of the individual's rights in relation to their personal data, which is in digital form or has been digitized subsequently. It further extends beyond the borders in case processing of personal data occurs outside of India, as regards goods or services being provided to persons located in India.

There was an imminent requirement to curb the escalating concerns surrounding data breaches, unauthorized data exchange, and the absence of robust regulations surrounding the processing of personal data of individuals. The enactment of the DPDPA seems to be a positive step taken by the government to address such concerns. While the rules under the DPDPA are yet to be released in the public domain (which will elaborate more on the manner of compliances), the DPDPA (in its current form) seems like an attempt by the government to strike a balance to safeguard the rights of individuals on one hand and at the same time ensuring that corporate entities are not overburdened with compliances.

Governing Data Protection Legislation

2.1. Overview of principal legislation

From 2011 to 2023, India had only a very basic dedicated legislation covering the arena of data protection and data privacy. This piece of legislation was called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") , which was framed under the Information Technology Act, 2000 ("IT Act"). It is only in 2023 that the Central Government enacted the DPDPA, thereby re-hauling and introducing a more comprehensive data protection legislation.

2.2. Additional or ancillary regulation, directives, or norms

The regulatory landscape for data protection in India is additionally supplemented by several other laws (which are sector-specific). These legislations include Information Technology (the Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013, and the Consumer Protection (E-Commerce) Rules, 2020. Further, the Reserve Bank of India (RBI) has also prescribed a set of comprehensive guidelines for the handling of personal data by banking and financial service institutions.

2.3. Upcoming or proposed legislation (if applicable)

The DPDPA, pursuant to its enactment, will become the principal legislation governing the laws relating to data protection in India. The DPDPA was passed with the objective of providing an effective and robust mechanism for the protection of personal data. While the statute has been enacted and published in the official Gazette, it is yet to be notified (subsequent to which it will come into force). Further, the rules under the statute are also yet to be released in the public domain, which will provide for the detailed manner in which compliance will be required to be observed.

Scope of Application

3.1. Legislative Scope

3.1.1. Definition of personal data

As per the DPDPA, Data means, 'a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means'. The Act further lays down that any data with which a person is directly or indirectly identifiable is referred to as 'personal data'.

3.1.2. Definition of different categories of personal data

It is pertinent to note that the DPDPA applies to the processing of digital personal data, wherein the data has been collected in a digital form, or in a non-digital form, but has been digitized subsequent to collection. Thus, the DPDPA excludes the data collected in a non-digitized form (which is not digitized subsequently) from its ambit.

3.1.3.Treatment of data and its different categories

- Regulation of personal and non-personal data

The DPDPA does not apply to personal data that is processed for the purpose of any personal or domestic use by an individual. It has been further laid down that it also does not apply to any data that has been made available to the public by either the Data Principal or any other person obligated to do so under any law.

- Regulation of electronic and non-electronic data

The DPDPA provides for the regulation of data that is collected in electronic and non-electronic form that is subsequently digitized. However, it does not regulate data that is collected in non-electronic form, and isn't digitized subsequently.

3.1.4. Other key definitions pertaining to data and its processing

Other key definitions pertaining to Personal Data and its processing include:

a)Personal Data Breach - Any data that is subjected to unauthorized processing, which also includes accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data would be regarded as a breach of personal data.

b)Processing - Processing of personal data is considered as an operation or set of operations which is performed on digital personal data, such as collection, recording, storage, organizing of data, etc.

3.2. Statutory exemptions

The DPDPA provides for certain exemptions wherein the Data Fiduciaries are exempt from specific obligations. These exemptions include instances where processing is essential for legal enforcement or by judicial bodies, for investigation, or processing data of Data Principals outside India based on contractual agreements. Moreover, the law permits the Central Government to exempt state instrumentalities from compliance in the interest of national sovereignty, security, public order, or international relations. It also exempts data processing for research, archival, or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is conducted according to prescribed standards. Additionally, the government has the authority to exempt certain categories of entities from specific obligations outlined in the provisions related to notice, data processing for decision-making, erasure, additional obligations, and access to personal data.

3.3. Territorial and extra-territorial application

The DPDPA applies to the processing of personal data within the territory of India as well as the processing of personal data outside India (irrespective of where the Data Fiduciary is located) if such processing is in connection with any activity related to the offering of goods or services to Data Principals located within India.

Legislative Framework

4.1. Key stakeholders

The following are the key stakeholders as per the DPDPA:

1. Data Fiduciary – Any individual or entity who is responsible for determining the purpose of processing of personal data.

2. Significant Data Fiduciary - The central government may notify a Data Fiduciary as a significant data fiduciary based on certain factors, which may include volume and sensitivity of personal data processed, risk to the right of the Data Principal, security of the state, etc.

3. Data Principal - A person whose personal data is being collected for processing. The DPDPA also provides for a condition where, in case the individual is a child, the definition of Data Principal would further extend to its parents or legal guardians. Further, in the case of a disabled person, the definition may extend to its lawful guardian.

4. Data Processor - A person who processes the personal data of the Data Principal on behalf of the Data Fiduciary.

5. Consent Manager - A person who serves as a single point of contact for facilitating the process through which a Data Principal can provide, handle, assess, and retract their consent as regards their personal data.

4.2. Role and responsibilities of key stakeholders

A Data Fiduciary is responsible for processing personal data after complying with some primary prerequisites, which include obtaining valid consent and giving notice regarding the same to the Data Principal. As regards the Data Principal, it is their duty to comply with legal requirements while providing verifiable, authentic information. Further, they should ensure that they never file a false or misleading grievance/complaint.

Further, it is pertinent to note that a Significant Data Fiduciary is required to additionally undertake certain obligations (in addition to the responsibilities undertaken by a Data Fiduciary), which include appointing a 'Data Protection Officer'.

As regards the Consent Manager, they play an important role in standardizing the consent management process for a Data Fiduciary. Consent Managers shall be accountable to the Data Principals and shall act on their behalf, subject to obligations which will be prescribed by the Government.

Requirements for Data Processing

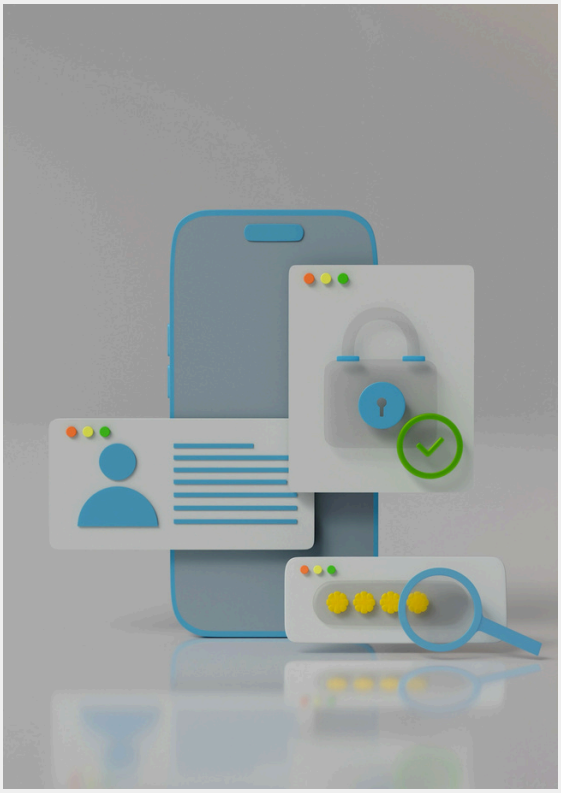
5.1. Grounds for collection and processing

- Consent

A Data Fiduciary is required to obtain consent from the Data Principal before collecting Personal Data for the specified purposes and legitimate uses.

- Consent Notice

The Data Fiduciary is obligated to furnish a notice to the Data Principal, comprehensively detailing crucial



information (the manner of which shall be prescribed in the rules). This notice should explicitly outline:

a. the personal data and the purpose for which the same is proposed to be processed.

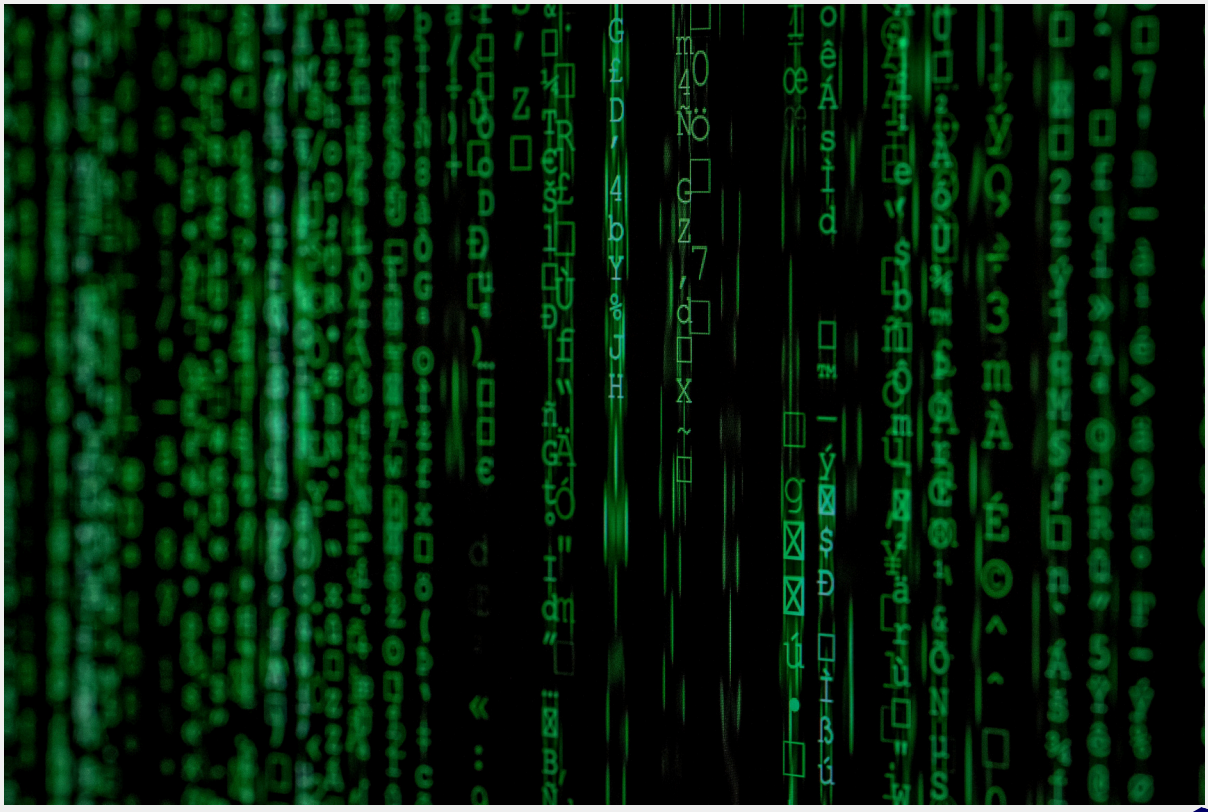
b. the manner in which she may exercise her rights.

c. the manner in which the Data Principal may make a complaint to the Board.

Further, the Data Principal needs to ensure that the consent must be freely given, specific, fully informed, unconditional, and unambiguous, requiring a clear affirmative action from the Data Principal. It is crucial that the request for consent and any related information or communication presented to the Data Principal is conveyed in a language that is clear and easily comprehensible. Additionally, it must be ensured that the Data Principal can access the request and related information in either English or any other language specified in the Eighth Schedule to the Constitution of India.

- Withdrawal of Consent

It has been further specified that while the consent is the basis of processing of the personal data, the



Data Principal shall also be given the right to withdraw consent at any point in time as easily as the consent was given. However, as regards the withdrawal, it has been further specified that "such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal". Moreover, such a withdrawal makes it mandatory for the Data Fiduciary to end the processing of the personal data of the Data Principal (unless specifically provided by the DPAPA).

5.2. Data storage and retention timelines

While no specific timelines have been prescribed for the retention of personal data, a Data Fiduciary is required to store personal data of the Data Principal only for specified purposes, which indicates that as soon as the specified purpose is over, the personal data shall not be retained.

5.3. Data correction, completion, updating, or erasure of data

Upon withdrawal of consent by the Data Principal (even before the completion of the specified purpose of the data collected), the Data Fiduciary and its Data Processors shall erase or cease to process the personal data of the Data Principal within a reasonable time (which is yet to be specified by the rules). Further, the Data Principal can request corrections, completion of missing information, or updates to any inaccurate or incomplete data held by a Data Fiduciary.

5.4. Data protection and security practices and procedures

As a general obligation, the Data Fiduciary is mandated to implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.

5.5. Disclosure, sharing, and transfer of data

As regards the disclosure, sharing, or transfer of personal data of the Data Principal, the DPDPA provides that information regarding the extent and purpose of sharing of the personal data needs to be disclosed to the Data Principal, and consent for the same needs to be sought by way of a consent notice.

5.6. Cross-border transfer of data

The Central Government has the power to restrict the transfer of personal data by a Data Fiduciary for processing to specific countries or territories outside India by notifying the list of such countries.

5.7. Grievance redressal

A Data Fiduciary or the Consent Manager shall establish an effective and readily available mechanism to redress the grievances of Data Principals in case of any act or omission or regarding the performance of their obligations in relation to the personal data of such Data Principal.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

- Right to withdraw consent

The DPDPA recognizes the right to withdraw consent, in exercise of which, the Data Principal can withdraw consent previously provided for processing of their personal data for a specified purpose. It has also been specified that upon withdrawal of consent, the Data Fiduciary and its Data Processors shall cease to process the personal data of the Data Principal within a reasonable time. The ease of exercising the option to withdraw consent shall be comparable to the ease with which consent was originally given.

- Right to grievance redressal and appeal

A Data Principal shall have the right to a means of grievance redressal provided by a Data Fiduciary or a Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of his/her rights.

- Right to access information

The Data Principal can exercise their right to access the following information about their personal data:

(1) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(2) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(3) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

- Right to nominate

A Data Principal has been conferred the right to nominate any other individual who can exercise the rights of the data principal in the event of death or incapacity of the Data Principal.

6.2. Duties

The Data Principals are required to perform, inter alia, the following duties:

a)to ensure not to impersonate another person while providing his/her personal data;

b)to ensure not to suppress any material information while providing his/her personal data for any document, unique identifier, proof of identity, or proof of address issued by the State or any of its instrumentalities;

c)to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and

d)to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure.

Processing of Children or Minors' Data

The DPDPA defines a 'child' as an "individual who has not completed the age of eighteen years". As regards processing of personal data relating to children, the DPDPA provides that before processing any personal data of a child, the Data Fiduciary shall obtain verifiable consent of the parent of such child. The DPDPA further provides for the following aspects as regards the processing of personal data of a child:

i. The Data Fiduciary shall not undertake such processing of personal data which is likely to cause a detrimental effect on the well-being of a child.

ii. The Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

The DPDPA provides for the formation of the Data Protection Board of India ("Board"), which shall inter alia be responsible for adjudication of any complaints with respect to breach of any provisions of the statute. The Board shall consist of a chairperson and such other members as the Central Government specifies.

8.2. Role, functions, and powers of authorities

- Role, functions, and powers of the principal data regulation authority

The DPDPA has prescribed that the Board shall have the following powers and functions:

a. on receipt of an intimation of personal data breach, to direct any urgent remedial or mitigation measures, and to inquire into such personal data breach and impose a penalty.

b. on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations or the exercise of rights by the Data Principal, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty.

c. on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to their personal data, to inquire into such breach and impose a penalty.

d. on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose a penalty.

e. on a reference made by the Central Government in respect of the breach by an intermediary, to inquire into such breach and impose a penalty.

The Board may also direct the parties to attempt resolution of the dispute through mediation.

- Role, functions, and powers of additional or ancillary data regulation authorities (if applicable)

N/A

8.3. Role, functions, and powers of civil/criminal courts in the field of data regulation

An appeal from an order of the Board will lie to the Telecom Disputes Settlement and Appellate Tribunal (which has been designated as the Appellate Board under the DPDPA) within a period of 60 days from the date of the order passed by the Board. The Appellate Tribunal has the power to either confirm, modify, or set aside the order passed by the Board. The DPDPA mentions that the Appellate Board shall endeavour to dispose of the appeal within six months from the date on which the appeal is presented to it. An appeal from the order of the Appellate Board will lie before the Supreme Court of India.

Consequences of non-compliance

9.1. Consequences and penalties for data breach

The DPDPA prescribes that any breach on the part of the Data Fiduciary to take reasonable security safeguards to prevent personal data breach could result in damages to the tune of INR 250 crores (approx. 33 million USD).

9.2. Consequences and penalties for other violations and non-compliance

The DPDPA also prescribes penalties for various other breaches of the provisions of the statute. These are listed as follows:

i. Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach – Up to INR 250 crores (approx. 33 million USD).

ii. Breach in observance of additional obligations in relation to children - Up to INR 200 crores (approx. 26 million USD).

iii. Breach in observance of additional obligations by a Significant Data Fiduciary - Up to INR 150 crores (approx. 20 million USD).

iv. Breach in observance of the duties by the Data Principal – Up to INR 1000 (approx. 33 USD 12).

v. Breach of any term of voluntary undertaking accepted by the Board – Up to the extent applicable for the breach in respect of which the proceedings were instituted

vi. Breach of any other provision of this Act (or the rules made thereunder) - Up to INR 50 crores (approx. 7 million USD).

Conclusion

The enactment of the DPDPA has been a major positive development in India in the field of data protection. While the statute is yet to be officially notified (after which it will come into force), businesses in India have already started the process of putting in place policies and mechanisms for observing compliance with the provisions of the statute. The enactment of this statute has put India at par with other nations in terms of having a robust data protection legislation. Further, the magnitude of penalties (which are much higher than the GDPR) will ensure that businesses will take concrete steps to ensure that they are compliant with the provisions of the statute.

Contact Us

+91-11-41023400

www.ahlawatassociates.com

gaurav.bhalla@ahlawatassociates.in

Plot No. 66, LGF
#TheHub, Okhla Phase III, Okhla Industrial Estate
New Delhi, 110020 India

Portugal

Introduction

Concerns raised on the subject of cybersecurity and data protection are closely linked to rapid technological advances and the increasing digitalization of society. Indeed, the collection and storage of data by digital means, as well as the widespread use of technological devices, are everyday realities that bring not only great benefits and conveniences but also ever-increasing responsibilities and challenges. In effect, the collection of large amounts of information by digital means (including personal and sensitive data) poses a particular challenge to the entities that collect it, particularly concerning the security of such data, which is increasingly subject to possible cyber-attacks.

Data protection legislation in Portugal is aligned with European Union law, in particular with the General Data Protection Regulation ("GDPR" – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), whose execution in Portugal was ensured by the Personal Data Protection Law ("PDPL" – Law No. 58/2019, of 8 August 2019).

In Portugal, the Constitution of the Portuguese Republic provides for the protection of personal data and other data whose safeguarding is justified by reasons of national interest, being the National Data Protection Commission ("CNPD") the entity responsible for monitoring and enforcing compliance with data protection legislation.

According to the GDPR, personal data means any information relating to an identified or identifiable natural person ("data subject"). Taking into account that such personal data can be used to identify a person – either directly or indirectly –, it is therefore essential to guarantee the privacy and security of this data, to protect the rights, freedoms, and guarantees of natural persons.

This paper explores the legal panorama of personal data protection in Portugal, highlighting the main differences in relation to the GDPR, as well as the rights of data subjects, the responsibilities of organizations that handle personal data, and the consequences of violating data protection legislation.

Contact Us

+ 351 213 595 090

www.mgra.pt

hlr@mgra.pt

Avenida 5 de Outubro, 16, Floor 3
Lisbon, 1050-056 Portugal

GOVERNING DATA PROTECTION LEGISLATION

II.1. Overview of principal legislation

In Portugal, personal data protection is primarily provided for, within the scope of fundamental rights, in Article 35 of the Constitution of the Portuguese Republic, which establishes that the law defines the appropriate forms of protection of personal data and other data whose safeguarding is justified for reasons of national interest. In addition, data protection legislation is also governed by the PDPL, which ensures the execution of the GDPR in the Portuguese legal system. The GDPR establishes the framework and rules of the European Union law on the protection of natural persons concerning the processing of personal data and on the free movement of such data. It should be noted that the GDPR became applicable from 25 May 2018 and it is binding in its entirety and directly applicable in all Member States (including Portugal), under the terms of Article 288 of the Treaty on the Functioning of the European Union, and Article 99/2 of the GDPR. In other words, the GDPR embodies the European Union's effort to strengthen and unify data protection laws across all the EU Member States.

Other relevant laws in Portugal, besides the PDPL, are listed below:

- Law no. 59/2019, of 8 August 2019, regarding personal data for the prevention, detection, investigation, or prosecution of criminal offences;
- Law no. 41/2004, of 18 August 2004 (as amended), regarding personal data protection and privacy in telecommunications;
- Law no. 43/2004, of 18 August 2004 (as amended), regarding the organisation and operation of the National Data Protection Commission ("CNPD").

II.2. Additional or ancillary regulation, directives, or norms

In addition to the GDPR and the aforementioned Portuguese legislation, there are additional regulations, directives, and standards that can be relevant to data protection in Portugal.
The CNPD (independent and public supervisory authority established in Portugal under Article 51 of the GDPR) is responsible for monitoring the application of the GDPR to defend the fundamental rights and freedoms of natural persons regarding processing, and to facilitate the free movement of such data within the European Union. As part of its remit, the CNPD has drawn up regulations and directives, of which we would highlight:

- Regulation no. 798/2018, of 14 November 2018 (Regulation no. 1/2018 CNPD), approved under Articles 35(4) and 57(1)(k) of the GDPR, on the list of processing operations of personal data subject to a Data Protection Impact Assessment (DPIA);

- Regulation no. 834/2021, of 14 April 2021, approved under Articles 43(1)(b), 43(3) and 57(1)(p) of the GDPR, on additional accreditation requirements for certification bodies in relation to ISO/IEC 17065/2012;

- Directive no. 2022/1, of 25 January 2022, on electronic direct marketing communications;

- Directive no. 2023/1, of 10 January 2023, on organisational and security measures applicable to the processing of personal data.

Furthermore, organizations can adopt internationally recognized technical standards and best practices to ensure the security and privacy of data. For example, the ISO/IEC 27001 standard serves as an international benchmark specifying the requirements for an Information Security Management System (ISMS)
.
ISO/IEC 27001 aims to encompass measures for the implementation, operation, monitoring, review, and continuous improvement of the ISMS. This includes identifying information security risks, implementing appropriate security measures, establishing security policies and procedures, and conducting regular audits and assessments to ensure compliance with the standard's requirements.

Certification in compliance with ISO/IEC 27001 is internationally recognized and demonstrates an organization's commitment and concern regarding information security. It enhances trust among customers, partners, and stakeholders, while also ensuring compliance with legal and regulatory requirements related to the protection of personal data and privacy

SCOPE OF APPLICATION

III.1 Legislative Scope

III.1.1 Definition of personal data

The GDPR definition of personal data is applicable in Portugal: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" – cf. Article 4(1) of the GDPR. Therefore, personal data shall cover information such as a person's name, home address, email address, identity card number, biometric data (fingerprints or facial features), location data, genetic data, and online identifiers (IP address or cookies).

In other words, any information that can be used, either alone or in combination with other information, to identify a natural person is considered personal data and is subject to data protection legislation in Portugal, in particular, and from the outset, to the PDPL.

III.1.2 Definition of different categories of personal data

In Portugal, as well as in the GDPR, personal data is categorized into different types depending on its sensitivity and nature.

Article 9(1) of the GDPR establishes a general prohibition on the processing of special categories of sensitive personal data, namely those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation. Without prejudice, this prohibition does not apply if one of the exceptions provided for in the GDPR is met (cf. Article 9(2)(a)-(j) GDPR). As a rule, the processing of this kind of personal data, where permitted, is generally subject to stricter criteria of protection and/or consent.

Special cases of data processing also include personal data relating to children (Article 8 GDPR and Article 16 PDPL), criminal convictions and offences (Article 10 GDPR) and deceased persons (Article 17 PDPL).

The PDPL also contains special provisions for specific situations, for example:

- Video surveillance, imposing limits on the incidence of cameras (Article 19 PDPL);
- Impossibility of exercising the rights to information and access to personal data (Articles 13-15 GDPR) when the law imposes a duty of secrecy on the controller or processor that is enforceable against the data subject (Article 20 PDPL);
- Articulation of the protection of personal data with the exercise of freedom of expression, information, and the press, including the processing of data for journalistic purposes and for the purposes of academic, artistic, or literary expression (Article 24 PDPL);
- Publication of personal data in official journals (Article 25 PDPL);
- Access to administrative documents and publication of data in the context of public procurement (Articles 26 and 27 PDPL);
- Processing of workers' personal data in the context of labour relations (Article 28 PDPL);
- Processing of health and genetic data (Article 29 PDPL);
- Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes (Article 31 PDPL).

Additionally, and as a general rule, personal data can also be categorized according to its nature, for example:

- Identification data (i.e., name, identification number, passport number and tax identification number);

- Contact information (i.e., email address, telephone number, and home address);
- Location data (i.e., GPS data and mobile device location data);
- Financial data (i.e., credit card information, bank account information, and financial transaction history);
- Health data (i.e., medical records, diagnoses, and treatments).

III.1.3 Treatment of data and its different categories

Ø Regulation of personal and non-personal data

Personal data is defined in Article 4(1) of the GDPR and consists of any information relating to an identified or identifiable person.

On the other hand, non-personal data sets refer to data that does not relate to an identified or identifiable natural person: in other words, anonymous data or data that has been subsequently anonymized and cannot be attributed or used to identify in any way a specific individual/natural person.

It should be noted, however, that mixed records contain both personal and non-personal data (i.e., company tax records that include the name and telephone number of the company's director). In most cases, the personal and non-personal data in mixed data sets are inseparable, and if it is a mixed data set, it must therefore comply with the rules of the GDPR and the PDPL.

ØRegulation of electronic and non-electronic data

In Portugal, electronic and non-electronic data are primarily regulated by the GDPR and the PDPL, which establish rules for the processing of personal data, regardless of the format in which it is stored.

In the field of health and genetic data processing, Article29(2) PDPL establishes that in the cases provided for in Article 9(2)(h) and (i) of the GDPR, the processing of the data provided for in Article 9(1) of the GDPR must be carried out by a professional bound by secrecy or by another person subject to a duty of confidentiality, and appropriate information security measures must be guaranteed. Furthermore, access to such data shall be exclusively electronic, unless technically impossible or expressly stated otherwise by the data subject, and its subsequent disclosure or transmission shall be prohibited.

III.1.4 Other key definitions pertaining to data and its processing

Under the GDPR (see Article 4), there are several basic definitions relating to data and its processing, of which we highlight:

- Data subject: the natural person to whom the personal data relates;
- Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- Data processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;
- Data processing: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction;
- Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which, through a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- Personal data breach: 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.

These definitions are essential for understanding obligations and responsibilities in this field and, in turn, ensuring that the processing of personal data is carried out ethically.

III.2 Statutory exemptions

Data protection laws often provide for exemptions or exceptions to the processing of personal data in certain circumstances.

For example, certain legal obligations may require the processing of personal data without the consent of the data subject (i.e., to meet tax obligations, conduct criminal investigations, or comply with court orders).

In addition, data protection legislation may provide exemptions for the processing of personal data for journalistic, artistic, scientific, or cultural purposes, provided that it is carried out in accordance with ethical principles and fundamental rights.

There may also be exemptions for the processing of personal data for reasons of public interest in areas such as public health, public security, crime prevention, or protection against threats to public security.

However, the data controller, within the scope of these exemptions, is still required to ensure that the processing of personal data is fair, transparent, and proportionate to the specific purposes (in other words, subject to appropriate and specific measures to protect the rights and freedoms of natural persons).

III. 3 Territorial and extra-territorial application

As a general rule, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (Article 3(1) GDPR).

It should be noted that the GDPR may also apply to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union (Article 3(2) GDPR) and/or to the processing of personal data by a controller not established in the Union (Article 3(3) GDPR).

In its turn, the PDPL applies to the processing of personal data conducted within Portugal, regardless of the public or private nature of the controller or processor, even if the processing of personal data is carried out in fulfilment of legal obligations or in the pursuit of public interest missions, with all the exclusions provided for in Article 2 of the GDPR applying.

Regarding the extra-territorial application, the PDPL also applies to the processing of personal data carried out outside Portugal when:

- It is carried out within the scope of the activity of an establishment located in Portugal; or
- It affects data subjects who are in Portugal when the processing activities are subject to Article 3(2) of the GDPR; or
- It affects data registered in the consular offices of Portuguese nationals residing abroad.

Legislative Framework

IV. 1 Key stakeholders

The data controller plays a central role in the context of personal data protection. The definition of data controller is given by the GDPR (Article 4(7) GDPR) and adopted by the PDPL: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In addition to the data controller, we find:

- The data subject (Article 4(1) GDPR): the natural person to whom the personal data relates and belongs; both the GDPR (Article 12 and following GDPR) and the PDPL guarantee several rights to the data subjects, aiming to ensure that the data subjects have control over their personal data, and that such data is lawfully processed;

- The data processor (Articles 4(8) and 28 GDPR): the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; it should be noted that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject;

- The Data Protection Officer / "Encarregado de Proteção de Dados" ("DPO" / "EPD"): designated by the controller and/or processor in certain cases (Article 37(1) GDPR), it shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data (Article 38(1) GDPR). It should be emphasized that the DPO has specific tasks (Article 39 GDPR), such as:

    - Inform and advise the controller or the processor;

    - Monitor compliance with data protection legislation;

    - Provide advice where requested as regards the data protection impact assessment and monitor its performance;

    - Cooperate with the supervisory authority;

    - Act as the contact point for the supervisory authority on issues relating to processing.

In this regard, the PDPL specifies the criteria laid down in the GDPR and also assigns specific duties to the DPO (Articles 9-15 PDPL).

IV.2 Role and responsibilities of key stakeholders

The data subject shall decide how its personal data is processed and handled, and has several rights, such as

the right to confirm whether the data is being processed and, if so, to have access to that data and information. Where applicable, the data subject may also: (i) request that inaccurate or incomplete personal data be corrected; (ii) request the deletion of personal data, unless there are legal grounds for its processing; (iii) object to the processing of personal data in certain circumstances, such as in direct marketing situations; (iv) request the restriction of the processing of personal data in certain specific situations.

In its turn, the data controller must (i) ensure that the processing of personal data is carried out in accordance with the provisions of the GDPR and national data protection legislation; (ii) define the specific purposes for which personal data are processed and (iii) ensure that the rights of data subjects are respected, including the rights of access, rectification, erasure and portability. The controller should also implement appropriate technical and organizational measures to ensure the security and privacy of personal data.

The data processor shall implement technical and organizational measures to ensure compliance with data protection laws (i.e., GDPR and national laws), and shall also manage the storage of personal data on servers or cloud platforms and process personal data on behalf of the data controller (i.e., payment processing and marketing services). Therefore, it is crucial for the controller to select processors who provide sufficient guarantees regarding the implementation of appropriate security measures and compliance with data protection laws. A formal contract should be established between the two parties, clearly defining the obligations, responsibilities, and security measures that the processor must adopt to protect personal data. The parties shall work together to ensure that personal data is processed in accordance with data protection laws and regulations (Article 28 GDPR).

REQUIREMENTS FOR DATA PROCESSING

V.1. Grounds for collection and processing

The processing of personal data is delimited by principles such as (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimization, (iv) accuracy, (v) storage limitation, and (vi) integrity and confidentiality. The controller is subject to accountability and shall be responsible for, and be able to demonstrate compliance with, such principles.

Processing of personal data shall be lawful only if and to the extent that at least one of the following applies (Article 6(1) GDPR):

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes;

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- Processing is necessary for compliance with a legal obligation to which the controller is subject;

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

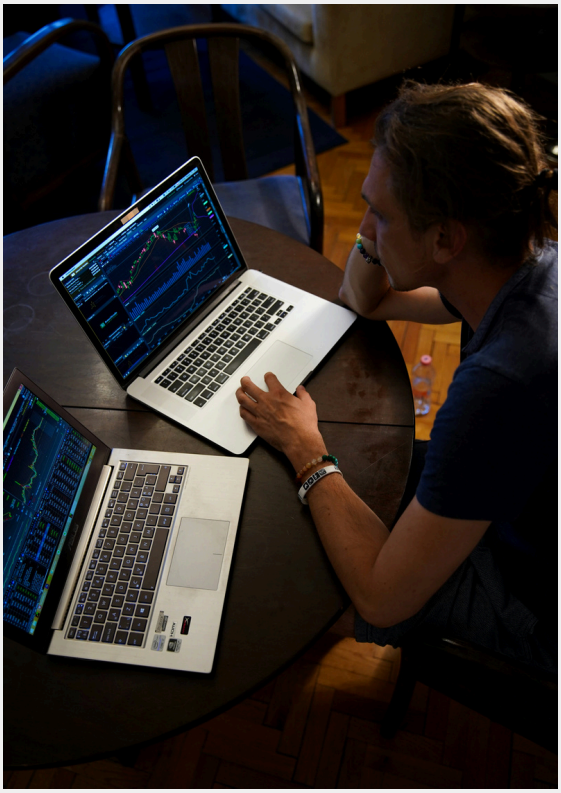
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (except if processing is carried out by public authorities in the performance of their tasks).

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his/her personal data. The data subject has the right to withdraw his/her consent at any time, and such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. If consent is withdrawn, the controller must stop processing the data subject's personal data for the specific purposes for which consent was withdrawn.

V.2. Data storage and retention timelines

One of the main principles of personal data processing is that of storage limitation (Article 5(1)(e) GDPR). The GDPR provides general guidelines for limiting the storage of personal data.

The storage and retention periods for personal data are determined based on several factors, including the purpose of the data processing, legal



requirements, industry-specific regulations, and an organization's internal policies.

In Portugal, the PDPL provides specific guidelines on the storage of personal data. As a general rule, the retention period for personal data is that which is set by law or regulation or, in the absence thereof, that which is necessary for the fulfilment of the purpose (Article 21(1) PDPL). Furthermore, when personal data is necessary for the controller or processor to prove the fulfilment of contractual or other obligations, it may be kept for as long as the corresponding rights are not time-barred. (Article 21(3) PDPL). It should also be emphasized that when the purpose for which personal data was initially or subsequently processed ceases, the controller must destroy or anonymize it (Article 21(4) PDPL).

V.3. Data correction, completion, updating or erasure of data

According to GDPR (Articles 12-23 GDPR), data subjects have several rights related to their personal data, framed in (i) information and access to personal data, (ii) rectification and erasure, (iii) right to object, and to not be subject to automated individual decision-making. Such rights, however, can be restricted (Article 23 GDPR).

In other words, data subjects have the right to correct, complete, update or even delete their personal data.

A data subject may request the rectification or update of inaccurate or incomplete personal data (i.e., inaccurate or out of date personal data) to ensure that it is accurate and reflects reality.

With respect to deletion, data subjects have the right to request the deletion of their personal data in certain circumstances (i.e., personal data is no longer necessary for the purposes for which it was collected, data subjects withdraw consent, or personal data is processed unlawfully).

The rights of the data subject may be restricted when such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, for example, national security, defence, or public security.

In particular, the right to erasure ("right to be forgotten") is restricted to the extent that processing is necessary for the exercise of the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims.
Organizations are required to provide mechanisms for data subjects to exercise their rights, usually through a process for requesting the correction, completion, updating, or deletion of personal data. This process should be easily accessible, and data subjects should not be subject to unjustified obstacles in exercising these rights.

V.4 Data protection and security practices and procedures

The security of processing of personal data is essential to ensure the privacy and integrity of the information of data subjects. Article 32(1) GDPR establishes that the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- *The pseudonymization and encryption of personal data;*
- *The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;*
- *The ability to restore the availability and access to personal data promptly in the event of a physical or technical incident;*
- *A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

Access to personal data should be limited to authorized individuals who need the information to perform their jobs. Access controls such as multi-factor authentication and monitoring of access activities should be implemented. In addition, security measures should be implemented on devices used to process or store personal data, including firewalls, anti-virus software, regular software updates, and restrictions on the installation of unauthorized applications.

Monitoring and auditing systems should be in place to detect and respond to suspicious or unauthorized activities related to the processing of personal data. In the event of an incident, it is important to develop response plans to effectively manage data security breaches in accordance with legal requirements.

In Portugal, the competent authority for accrediting data protection certification bodies is IPAC, I. P. (Article 14(1) PDPL), and the competent authority for drafting codes of conduct governing specific activities is CNPD (Article 15(1) PDPL).

V.5 Disclosure, sharing, and transfer of data

Disclosure, sharing, and transfer of personal data involve the communication or sharing of personal data between different parties, whether within the same organization or between different organizations.

In many cases, the disclosure, sharing or transfer of personal data requires the explicit consent of the data subject. In some situations, the disclosure or transfer of personal data may be necessary for the performance of a contract, to comply with a legal obligation, to protect the vital interests of the data subject, or for the performance of tasks carried out in the public interest or in the exercise of official authority.

Organizations must therefore implement appropriate security measures to protect personal data during disclosure, sharing, or transfer. This includes access controls, activity monitoring, and protection against unauthorized access. In addition, tests should be conducted to identify potential vulnerabilities or threats to data security during disclosure, sharing, or transfer.

In addition, where personal data is shared with third parties, organizations should enter into confidentiality agreements to ensure that personal data is treated in accordance with data protection laws.

V.6 Cross-border transfer of data

For the purposes of the GDPR, cross-border processing means either:

- Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or

- Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Cross-border transfer of personal data involves the transmission of personal information from one country to another. This type of transfer is common in a globalized world, where companies often have operations in multiple countries and may need to access personal data of individuals located in different legal jurisdictions.

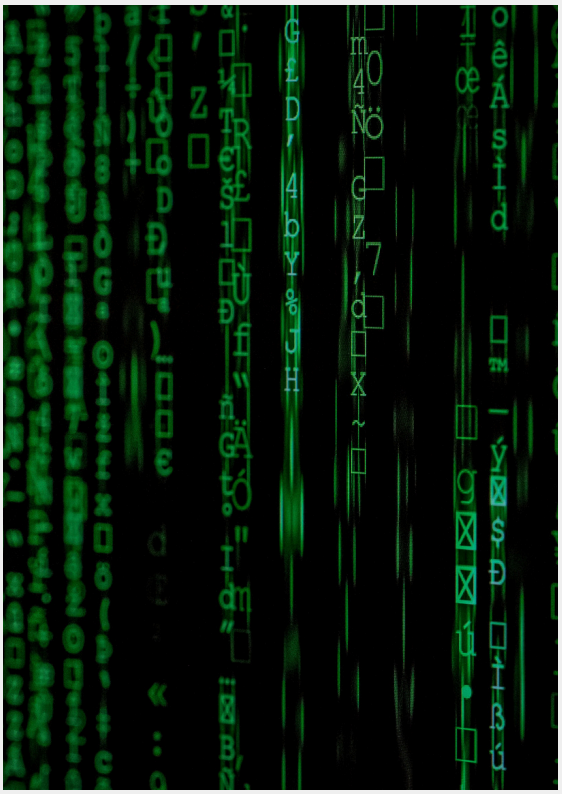
Transfers of personal data to third countries or international organizations is provided for in Articles 44 to 50 GDPR. As a general rule (Article 44 GDPR), any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in the GDPR are complied with by the controller and processor - including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

Article 49 GDPR also establishes derogations for specific situations: in the absence of an adequacy decision or of appropriate safeguards (including binding corporate rules), a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;



- The transfer is necessary for important reasons of public interest;

- The transfer is necessary for the establishment, exercise or defence of legal claims;

- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

- The transfer is made from a register which according to European Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest (only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case).

V.7 Grievance redressal

In Portugal, without prejudice to the right to lodge a complaint with the CNPD, any person may resort to means of administrative protection, namely of a petitionary or impugnatory nature, to ensure compliance with the legal provisions on the protection of personal data, under the terms of the Code of Administrative Procedure (Article 32 PDPL). Furthermore, any person who has suffered damage as a result of the unlawful processing of data or any other

act that violates the provisions of the GDPR or national law on the protection of personal data has the right to obtain compensation from the controller or processor for the damage suffered (Article 33 PDPL).

Additionally, complaints relating to personal data can be addressed to the CNPD (national authority responsible for monitoring and enforcing compliance with data protection legislation), which has, amongst other competences, the power to investigate complaints, carry out audits and impose sanctions in the event of infringements.

Complaints and claims shall be submitted in writing via the official website of the CNPD, by completing the complaint form with all relevant information.

Upon receipt of a complaint, the CNPD will investigate it and take the necessary measures to resolve the issue and ensure compliance with data protection laws (i.e., imposing sanctions on the organization that failed to comply with data protection laws).

RIGHTS AND DUTIES OF DATA PROVIDERS

VI.1 Rights and remedies

The rights of data subjects are provided for in Articles 12 and following of the GDPR and have no major changes in the PDPL. Data subjects have the rights of information and access to personal data, rectification and erasure of personal data, and to object and to not be subject to automated individual decision-making.

Data subjects also have the right to withdraw their consent to the processing of their personal data at any time. This means that they can revoke a previously given consent to the processing of their personal data. In addition, data subjects have the right to lodge a complaint with the CNPD if they believe that the processing of their personal data was made or is being made in breach of data protection legislation. Data subjects have the right to obtain information about how their personal data is processed, the purposes of the processing, how the data is used, and who has access to it.

In addition, data subjects can appoint a representative to act on their behalf and exercise their data protection rights if they are unable to do so personally. This can be particularly useful in situations where data subjects are unavailable or unable to act on their own behalf.

VI.2 Duties

The duties fall on data controllers and processors, which have several obligations set out in data protection legislation (i.e., GDPR and PDPL).

Data processing must comply with the principles set out in Article 5 GDPR (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality). The controller is responsible for, and shall be able to demonstrate compliance with such principles (accountability).

Purpose limitation and data minimization imply that data should be collected for specific, explicit, and legitimate purposes and should not be processed in a way that is incompatible with those purposes. In addition, data controllers must ensure that the data collected is necessary to achieve the specific purposes of the processing. When the purpose for which personal data were initially or subsequently processed ceases to exist, the controller must destroy or anonymize them.

They shall also provide data subjects with clear, concise, and easily accessible information about how their data is processed (i.e., through privacy policies, privacy notices or consent forms) and ensure data security by implementing appropriate technical and organizational measures to protect against unauthorized access, disclosure, alteration, accidental or unlawful destruction (in other words, personal data breaches).

Public or private organizations must also cooperate with the CNPD, providing it with all the information it requests in the exercise of its powers and competences.

On the other hand, the DPO is also subject to duties of secrecy and confidentiality.

Finally, the rights to information and access to personal data provided for in Articles 13 to 15 GDPR cannot be exercised when the law imposes a duty of secrecy on the controller or processor that is enforceable against the data subject; nevertheless, the data subject may request the CNPD to issue an opinion on the enforceability of the duty of secrecy (Article 20 PDPL).

PROCESSING OF CHILDREN OR MINORS' DATA

The processing of personal data of children or minors in Portugal is subject to specific provisions to ensure adequate protection, taking into account the vulnerability of these individuals.

The GDPR is directly applicable in Portugal and establishes that consent for the processing of personal data of children is only valid if the child is at least 16 years old. If the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

However, in Portugal, the personal data of children can only be processed on the basis of the consent provided for in Article 6(1)(a) GDPR and relating to the direct offer of information society services when they have reached the age of 13 (see Articles 8 GDPR and 16 PDPL). If a child is under 13, consent for the processing of his or her personal data must be given or authorized by his or her parents or legal guardians, preferably by means of secure authentication.

Therefore, children, as well as their parents or legal guardians, must be provided with clear and transparent information about how personal data will be processed. This includes the purposes of the processing, the categories of personal data involved, who has access to the data and how long the data will be kept.

These data must be treated with special care and protection, considering the vulnerability of a child. This includes implementing appropriate security measures to protect personal data from unauthorized access, disclosure or alteration, and ensuring that processing is transparent.

REGULATORY AUTHORITIES

VIII. 1 Overview of relevant statutory authorities

The CNPD is the national supervisory authority in Portugal for the purposes of the GDPR and the PDPL.

In addition to the provisions of Article 57 of the GDPR, the CNPD carries out other tasks, specifically provided for in Article 6 PDPL. Additionally, the CNPD also exercises the powers provided for in Article 58 of the GDPR. Under the terms of Article 43(1)(b) GDPR, the competent authority for accrediting data protection certification bodies is IPAC, I. P.

It should also be noted that any person, in accordance with the general rules, may bring actions before the administrative courts against the decisions, namely of an administrative offence nature, and omissions of the CNPD, as well as civil liability actions for the damage that such acts or omissions may have caused.

Other relevant authorities are the National Communications Authority (ANACOM), the Public Prosecutor's Office (MP), and the National Council for Ethics in the Life Sciences.

VIII. 2 Role, functions and powers of authorities

The CNPD is responsible for supervising and enforcing compliance with data protection

legislation. Its main functions include promoting the application of data protection laws, issuing guidelines and opinions, investigating complaints and data breaches, imposing corrective measures, and applying sanctions in the event of breaches. The CNPD also has investigative and supervisory powers, including the right to access information, request documents, conduct audits, and impose administrative sanctions such as warnings, fines, and data processing bans.

In addition to the provisions of Article 57 GDPR, the CNPD has the following duties:

- To give a non-binding opinion on legislative and regulatory measures relating to the protection of personal data, as well as on legal instruments under preparation in European or international institutions relating to the same matter;

- To monitor compliance with the provisions of the GDPR and other legal and regulatory provisions relating to the protection of personal data and the rights, freedoms, and guarantees of data subjects, and to correct and penalize non-compliance;

- Make available a list of processing operations subject to data protection impact assessment, pursuant to Article 35(4) GDPR, also defining criteria that make it possible to specify the notion of high risk provided for in that article;

- Prepare and submit to the European Data Protection Board draft criteria for the accreditation of code of conduct monitoring bodies and certification bodies, under the terms of articles 41 and 43 GDPR, and ensure the subsequent publication of the criteria, if approved;

- Co-operate with the Portuguese Accreditation Institute, I.P. (IPAC, I.P.). in relation to the application of the provisions of Article 14 PDPL, as well as in the definition of additional accreditation requirements, with a view to safeguarding consistency in the application of the GDPR.

Furthermore, CNPD exercises the powers laid down in Article 58 GDPR.

In addition to general data protection laws, there are specific laws that may affect data protection in certain sectors (i.e., the personal data and privacy protection in the electronic communications sector – Law no. 41/2004, of 18 August, as amended).

In this regard, ANACOM is responsible for the regulation and supervision of the electronic communications sector in Portugal, including data protection in certain contexts such as telecommunications and Internet services (i.e., ensuring the security of networks, electronic communications services, privacy in electronic communications and data protection in telecommunications services).

In addition to these authorities, other bodies may have a relevant role in data protection in Portugal, such as the Public Prosecutor's Office, which investigates cases of serious breaches of data protection, and the National Council for Ethics in the Life Sciences, which can provide opinions on ethical issues related to the processing of personal data in the context of health and biomedical research.

VIII. 3 Role, functions and powers of civil/criminal courts in the field of data regulation

In Portugal, without prejudice to the right to lodge a complaint with the CNPD, any person may resort to means of administrative protection, specifically of a petitionary or impugnatory nature, to ensure compliance with the legal provisions on the protection of personal data, under the terms of the Code of Administrative Procedure.
In addition, in the field of civil liability, any person who has suffered damage as a result of the unlawful processing of data or any other act that violates the provisions of the GDPR or national law on the protection of personal data has the right to obtain compensation from the controller or processor for the damage suffered.

Thus, in general, any person can bring actions against the CNPD's decisions, namely of an administrative offence nature, and omissions, as well as civil liability actions for the damage that such acts or omissions may have caused. Such actions fall within the jurisdiction of the administrative courts.

On the other hand, the data subject may bring actions against the controller or processor, including civil liability actions.

In cases of serious breaches, criminal courts may have to prosecute and judge the person(s) and or/organization(s) responsible. This includes cases of illegal access to information systems, unauthorized disclosure of personal data and other forms of cybercrime related to privacy and data protection.

Overall, civil and criminal courts play a crucial role in enforcing data protection laws in Portugal, ensuring that data subjects have effective remedies in case of violations of their rights and that those responsible for such violations are held accountable according to the law.

CONSEQUENCES OF NON-COMPLIANCE

IX.1 Consequences and penalties for data breach

According to Article 4(12) GDPR, a 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.

The most serious violations of personal data are classified in the PDPL as criminal offences (i.e., improper access, misappropriation, corruption or destruction of data – Articles 47 to 49 PDPL).

Other violations of personal data are classified as very serious or serious administrative offences (Articles 37 and 38 PDPL). The fines for these offences vary depending on the nature of the offender (natural or legal person) and its size (in the case of legal persons). In the case of legal persons, very serious offences can range from €2000 to €20.000.000, or 4% of annual worldwide turnover, whichever is higher, while serious offences can range from €1000 to €10.000.000, or 2% of annual worldwide turnover, whichever is higher.

Furthermore, organizations that do not comply with the GDPR and or the PDPL may be required to take corrective action to remedy the breach and mitigate any harm caused to data subjects. This may include implementing measures to protect the affected data, notifying data subjects of the breach and, where appropriate, providing compensation for any material or non-material damage. Additionally, they may be subject to the mentioned criminal and administrative offences typified by law.

The CNPD has the power to issue warnings and impose administrative fines on organizations that violate data protection laws. The CNPD may also intervene in legal proceedings in the event of a breach of the provisions of the GDPR and the PDPL, and must report to the Public Prosecutor's Office any criminal offences of which it becomes aware, in the performance of its duties or on account thereof, as well as carry out any necessary and urgent precautionary acts to secure evidence.

IX.2 Consequences and penalties for other violations and non-compliance

In addition to administrative sanctions, the person(s) and/or organization(s) that violate(s) data protection legislation may face civil actions brought by affected data subjects seeking compensation for damages caused by the breach and or non-compliance with the GDPR and or the PDPL. Additionally, the data subject has always the right to lodge a complaint with the CNPD.

Depending on the nature and severity of the breach and or non-compliance, regulatory authorities may end up revoking or suspending an organization's licenses and authorizations to operate in certain sectors, such as telecommunications, financial services or healthcare.

It should be noted that the PDPL does not make a profound distinction between data breaches (in the strict sense) and other breaches of the GDPR or the PDPL, treating data breaches (in the broad sense) as a unitary issue.

Therefore, and in summary, data breaches in Portugal can lead to various consequences and sanctions, including criminal investigations and judgements, administrative and or civil legal actions, administrative fines, reputational damages, loss or suspension of licenses, and complaints to the CNPD as well.

Conclusion

In the European Union and in Portugal, the protection of personal data is governed by specific legislation such as the GDPR and the PDPL, amongst others. The CNPD is the independent and public supervisory authority set up in Portugal under Article 51 of the GDPR, primarily responsible for monitoring and enforcing compliance with such legislation.

Personal data is protected and framed within the scope of fundamental rights and data subjects have several rights, including the right of access, rectification, erasure, restriction of processing, data portability and the right to object to the processing of their personal data. If an unforeseen event occurs, data subjects should file a complaint with the CNPD or resort to courts to ensure that their rights are respected and/or repair the damage caused.

Data controllers and processors handling personal data in Portugal have clear obligations to comply with data protection legislation (notably GDPR and PDPL), including by implementing appropriate technical and organizational measures to ensure the security and privacy of the data, under penalty of severe sanctions in case of violation.

Contact Us

+ 351 213 595 090

www.mgra.pt

hlr@mgra.pt

Avenida 5 de Outubro, 16, Floor 3
Lisbon, 1050-056 Portugal

Romania

Introduction

PETERKA & PARTNERS is a modern, independent, and integrated CEE full-service law firm with worldwide activities and a leader on the regional market. The law firm benefits from unique coverage across the CEE region, operating 100% fully-owned offices in the Czech Republic, Slovakia, Poland, Hungary, Bulgaria, Romania, Ukraine, Croatia, and Slovenia.

PETERKA & PARTNERS opened its Romanian office in 2010, strengthening the position of the firm in the CEE region and helping clients expand their businesses into a key market.

The Romanian team of PETERKA & PARTNERS consists of experienced and business-oriented lawyers with extensive knowledge of Romanian law and industry insight ,and provides domestic and international clients with complex legal services in all business law areas, from day-to-day assistance to sophisticated transactions, with a focus on Corporate and M&A, Labour Law, Real Estate, General Commercial and Distribution, Litigation and Insolvency, Compliance and Regulatory, Banking and Finance, E-Commerce, and Tax.

The Bucharest office assists clients active in a wide range of industries, including Automotive, Aviation, Retail and Luxury, Energy, IT&C and Technology, Pharma and Life Sciences, and Transportation and Logistics.

All of our lawyers are registered with the Romanian Bar Association and are fluent in English; part of the team may assist in French as well.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), as implemented by Law 190/2018, is the principal data protection legislation in Romania.

Contact Us

+40 21 310 48 82

www.peterkapartners.com/en/local/bucharest/

ciupala@peterkapartners.ro

33 Aviatorilor Boulevard,2nd floor, 1st District
Bucharest, 011853 Romania

The collective citation of these pieces of legislation used hereafter will be "Romanian Data Protection Acts".

Law 129/2018, completing Law No 102/005 on the establishment, organization, and functioning of the National Supervisory Authority for Personal Data Processing repealed the previous laws, Law 667/2001 for the protection of individuals in regards to Personal Data Processing and the free circulation of such data, which regulated the data protection in Romania before the enactment of the GDPR.

In Romania, the following pieces of sectoral-specific legislation impact data protection:

- Law No. 146/2021 on electronic monitoring in judicial and executive criminal proceedings
- Law No 363/2018 on the protection of individuals concerning the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting, and combating criminal offences, or the execution of penalties, educational and security measures, and on the free movement of such data.
- Law No 506/2004 on the processing of personal data and the protection of privacy in electronic communications.

Please note that this Guide does not cover these laws, but instead focuses on the general rules applicable to Data Protection in Romania, highlighting, whenever applicable, the derogations as contained in Law 190/2018, which are permitted under the GDPR.

2.2. Additional or ancillary regulation, directives, or norms

The National Authority for the Supervision of Data Processing (ANSPDCP) is the Romanian supervisory authority that is responsible for monitoring the application of the GDPR, and has functions and powers related to the regulation of data processing, monitoring the fulfilment of legal obligations by personal data controllers, and investigation of violations of data subjects' rights, ex officio or upon the receipt of a complaint or referral.

In the exercise of its powers, the ANSPDCP shall issue binding decisions and instructions to public authorities and institutions, legal entities governed by private law, and any other bodies, as well as to natural persons whose activities fall within the scope of the legislation on the protection of individuals about the processing of personal data, hereinafter referred to as “entities”. Decisions and instructions of a regulatory nature are published in the Official Gazette of Romania.

The applicable decisions are:

- Decision No. 133 of 3 July 2018 approving the Procedure for the receipt and settlement of complaints
- Decision No. 161 of 9 October 2018 approving the Procedure for conducting investigations
- Decision No 174 of 18 October 2018 on the list of operations for which it is obligatory to carry out a personal data protection impact assessment

Relevant for the interpretation of GDPR concepts at the national level is the general guidance (including guidelines, recommendations, and best practices) issued by the European Data Protection Board (EDPB), which serves to clarify the core notions of the GDPR and promote a consistent understanding of EU data protection law. This guidance is routinely followed by the Romanian Data Protection Authority (ANSPDCP) when responding to requests for opinions submitted by controllers and processors from both the public and private sectors, as well as by other entities and individuals, on various aspects concerning the application of the GDPR and related regulatory frameworks.

In this context, a notable development is the adoption by the EDPB, at its June 2025 plenary session, of Guidelines No. 2/2024 on Article 48 GDPR, addressing data transfers to third countries, in their final form.

From a practical perspective, enforcement activity by the ANSPDCP in 2024 focused on online operators in the retail sector, largely in response to complaints from data subjects. Key compliance failures included the use of non-essential cookies without prior consent and the processing of personal data—such as telephone numbers—for direct marketing without a valid legal basis under Article 6(1)(a) GDPR. Sanctions ranged between RON 20,000 and RON 75,000 (approximately EUR 4,000–15,000), typically accompanied by corrective measures, such as the reconfiguration of cookie consent mechanisms.

2.3. Upcoming or proposed legislation (if applicable)

There is no upcoming or proposed legislation in Romania.

Scope of Application

3.1. Legislative Scope

As per the GDPR.

3.1.1. Definition of personal data

As per the GDPR.

3.1.2. Definition of different categories of personal data

As per the GDPR.

3.1.3. Treatment of data and its different categories

- Regulation of personal and non-personal data: As per the GDPR.
- Regulation of electronic and non-electronic data: As per the GDPR.

Specific Romanian regulations

Three situations of data processing are regulated separately from the provisions of the GDPR, namely:

- Processing a national identification number

The processing of a national identification number, along with the collection or disclosure of documents containing it, must adhere to specific safeguards implemented by the controller. These safeguards include:

a) Implementation of Appropriate Technical and Organizational Measures: The controller must establish and apply suitable technical and organizational measures. These measures serve to ensure compliance with the principle of data minimization, as well as to guarantee the security and confidentiality of the personal data processing.

b) Appointment of a Data Protection Officer (DPO): The controller is required to appoint a Data Protection Officer, responsible for overseeing and advising on compliance with data protection regulations.

c) Establishment of Storage Periods: The controller should define storage periods based on the nature of the data and the purpose of processing. Additionally, specific timeframes must be set for the deletion, or review for deletion, of personal data.

d)Regular Training: Persons involved in processing personal data under the direct authority of the controller or processor must undergo regular training. This training aims to ensure a comprehensive understanding of

- Processing of personal data in the context of employment relationships

Where monitoring systems by means of electronic communications and/or video surveillance are used at the workplace, the processing of personal data of employees for the purpose of the legitimate interests pursued by the employer is only permitted if the following conditions are met:

a) Balancing of Interests: The legitimate interests pursued by the employer must be duly justified, and these interests must outweigh the interests, rights, and freedoms of the data subjects (employees).

b) Full and Explicit Prior Information: The employer is required to provide employees with comprehensive and explicit information before initiating the monitoring systems. This ensures transparency regarding the purpose and scope of the data processing.

c) Consultation with Trade Union or Representatives: Before implementing monitoring systems, the employer must consult with the trade union or, where applicable, employees' representatives. This consultation is a crucial step in obtaining input and feedback from the workforce.

Exploration of Less Intrusive Alternatives: The employer must demonstrate that other, less intrusive methods of achieving the intended purpose have been considered and proven ineffective. This underscores the importance of exploring alternatives before resorting to more invasive monitoring systems.

d) Exploration of Less Intrusive Alternatives: The employer must demonstrate that other, less intrusive methods of achieving the intended purpose have been considered and proven ineffective. This underscores the importance of exploring alternatives before resorting to more invasive monitoring systems.

e) Proportionate Duration of Data Storage: The duration for which personal data is stored must be proportionate to the purpose of processing. Generally, this should not exceed 30 days, unless specific situations provided for by law or duly justified cases necessitate a longer storage period.

the obligations related to the processing of personal data.

- **Processing of personal data in the context of employment relationships**

Where monitoring systems by means of electronic communications and/or video surveillance are used at the workplace, the processing of personal data of employees for the purpose of the legitimate interests pursued by the employer is only permitted if the following conditions are met:

a) Balancing of Interests: The legitimate interests pursued by the employer must be duly justified, and these interests must outweigh the interests, rights, and freedoms of the data subjects (employees).

b) Full and Explicit Prior Information: The employer is required to provide employees with comprehensive and explicit information before initiating the monitoring systems. This ensures transparency regarding the purpose and scope of the data processing.

c) Consultation with Trade Union or Representatives: Before implementing monitoring systems, the employer must consult with the trade union or, where applicable, employees' representatives. This consultation is a crucial step in obtaining input and feedback from the workforce.

d) Exploration of Less Intrusive Alternatives: The employer must demonstrate that other, less intrusive methods of achieving the intended purpose have been considered and proven ineffective. This underscores the importance of exploring alternatives before resorting to more invasive monitoring systems.

e) Proportionate Duration of Data Storage: The duration for which personal data is stored must be proportionate to the purpose of processing. Generally, this should not exceed 30 days, unless specific situations provided for by law or duly justified cases necessitate a longer storage period.

- **Processing of personal data and special categories of personal data in the context of a task carried out in the public interest**

The processing of personal and special data necessary for the performance of a task carried out in the public interest shall be carried out with the establishment of the following safeguards by the controller or the third party:

a) implementation of appropriate technical and organizational measures to comply with the principles of the GDPR, in particular data minimization and the principle of integrity and confidentiality;

b) the appointment of a data protection officer;

c) the establishment of storage periods depending on the nature of the data and the purpose of the processing, as well as specific periods within which personal data must be deleted or reviewed for deletion;

3.1.4. Other key definitions pertaining to data and its processing

As per GDPR.

Specific Romanian regulations

The following are also defined:

- **"Authorities and public bodies"** – the Chamber of Deputies and the Senate, the Presidential Administration, the Government, ministries, other specialized bodies of central public administration, authorities and autonomous public institutions, authorities of local and county public administration, other public authorities, as well as institutions under their subordination/coordination. For the purposes of the law, religious entities and associations and foundations of public utility are assimilated to public authorities/organizations;

- **"National identification number"** – the number by which an individual is identified in certain record systems and which has general applicability, such as: personal identification number, series and number of the identity document, passport number, driver's license number, social security number;

- **"Remediation plan"** – annex to the finding and sanctioning minutes of the offence, by which the National Supervisory Authority for Personal Data Processing establishes measures and a remediation deadline;

- **"Remediation measure"** – a solution ordered by the national supervisory authority in the remediation plan for the fulfillment by the public authority/organization of the obligations provided by law;

- **"Remediation deadline"** – a period of up to 90 days from the date of communication of the finding and sanctioning minutes

- of the offence, during which the public authority/organization has the opportunity to remedy the identified irregularities and fulfil legal obligations;

- **"Performing a task serving a public interest"** – includes activities of political parties or organizations of citizens belonging to national minorities, non-governmental organizations, serving the achievement of objectives provided by constitutional law or international public law, or the functioning of the democratic system, including encouraging citizen participation in the decision-making process and policy preparation, respectively promoting the principles and values of democracy.

3.2. Statutory exemptions

As per GDPR.

Specific Romanian regulations

There are two exemptions from the GDPR rules, namely ***in the processing of personal data for journalistic purposes or for purposes of academic, artistic, or literary expression*** when the processing relates to personal data which have been manifestly made public by the data subject or which are closely linked to the public status of the data subject or to the public nature of the facts in which it is involved ***and in the processing of personal data for scientific or historical research purposes, for statistical purposes or for archiving purposes in the public interest*** when the derogation is necessary to achieve those purposes.

3.3. Territorial and extra-territorial application

As per GDPR.

Legislative Framework

4.1. Key stakeholders

As per GDPR.

4.2. Role and responsibilities of key stakeholders

As per GDPR.

Requirements for Data Processing

5.1. Grounds for collection and processing

As per GDPR.

5.2. Data storage and retention timelines

As per GDPR.

5.*3. Data correction, completion, data updating, or erasure of data*

As per GDPR.

5.*4. Data protection and security practices and procedures*

As per GDPR.

Specific Romanian regulations

To ensure an increased level of security in employer-employee relations, Romanian legislation has also introduced the obligation that where monitoring systems are used by means of electronic communications and/or by means of video surveillance at the workplace, the processing of employees' personal data, for the purpose of achieving the legitimate interests pursued by the employer, is allowed only if the duration of storage of personal data is proportionate to the purpose of the processing, but not for more than 30 days, except in situations expressly regulated by law or in duly justified cases. So, if the employer wants to carry out surveillance by video or electronic means, it must delete the stored data after a maximum of 30 days from the date of storage.

5.5. Disclosure, sharing, and transfer of data

As per GDPR.

5.6. Cross-border transfer of data

As per GDPR.

5.7. Redressal of grievances

As per GDPR.

Specific Romanian regulations

Any data subject who believes that the processing of their personal data violates the applicable legal provisions has the right to complain. This applies particularly if the alleged breach occurs within Romania or affects the data subject's habitual residence or place of work. Complaints must be submitted in writing, either in Romanian or English, and sent to the supervisory authority. The supervisory authority shall inform the data subject of the admissibility of the complaint within 45 days of registration at the latest. If the authority finds that the information in the complaint is incomplete or insufficient, it may request that the data subject provide additional details for the complaint to be considered admissible for investigation. The National Supervisory Authority is then obligated to update the data subject on the progress or outcome of the investigation within 3 months from the date of informing the complainant that the complaint is admissible.

In addition to filing a complaint with the supervisory authority, data subjects also have the right to address their complaint directly to the competent court to defend their rights as guaranteed by applicable law. Where a legal claim has been brought with the same subject matter and same parties, the supervisory authority may order the suspension of, and/or close, the complaint, as appropriate. The data subject will have to inform the Authority, via a complaint form, of the lodging of such a complaint with the court.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

As per GDPR.

6.2. Duties

As per GDPR.

Processing of the data of Children or Minors

As per GDPR.

Specific Romanian regulations

The processing of the personal data of a child carried out on the basis of consent is lawful only when the child is at least 16 years of age. If the child is under the age of 16, such processing is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

As per GDPR.

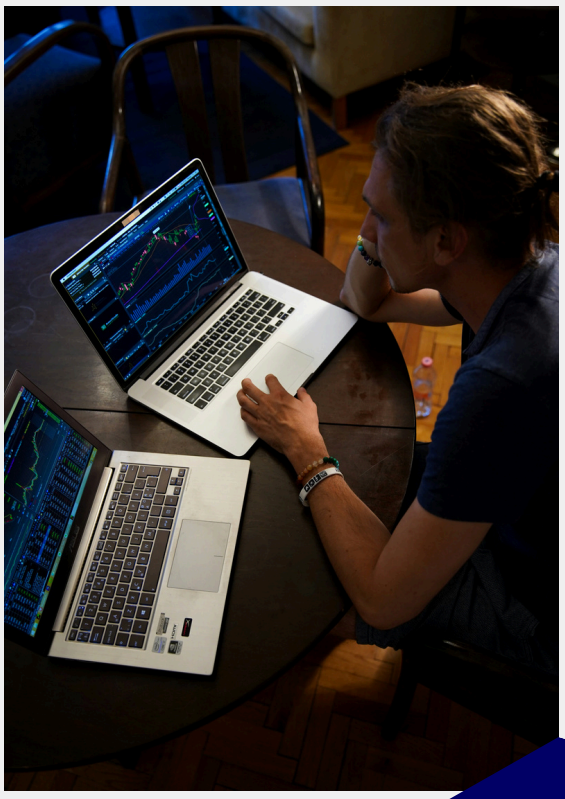
Specific Romanian regulations

The National Supervisory Authority for Personal Data Processing, hereinafter referred to as the National Supervisory Authority, is a public authority with legal personality, autonomous and independent from any other authority of the public administration, as well as from any natural person or legal entity in the private sector, which exercises the powers conferred to it by the legal provisions on the processing of personal data and the free movement of such data.

8.2. Role, functions, and powers of authorities

- **Role functions and powers of principal data regulation authority**

In Romania, the data regulation authority is the National Supervisory Authority for Personal Data Processing.



Romania

The objective of the National Supervisory Authority is to protect the fundamental rights and freedoms of natural persons, and in particular their right to private, family and private life, in relation to the processing of personal data and the free movement of such data.

Among the main tasks of the National Supervisory Authority for Personal Data Processing and its President, established in accordance with the GDPR, are:

- monitoring the uniform application of personal data protection legislation by all entities acting as data controllers;
- regulation, through the drafting of binding decisions and instructions, which are published in the Official Gazette of Romania;
- endorsement of draft legislation on personal data protection;
- guidance, through advisory activity, including to Parliament, the Government and other public authorities or institutions, and to entities acting as data controllers, and informing data subjects and the public of their obligations under the legislation on personal data protection and the rights guaranteed by law;
- monitoring the fulfilment of legal obligations by personal data controllers, through powers to investigate violations of data subjects' rights, ex officio or upon receipt of a complaint or referral;
- applying corrective measures in cases where breaches of the relevant legislation are found;
- cooperation and mutual assistance with the supervisory authorities of the other Member States, as well as cooperation with the European Commission and the European Data Protection Board, in the framework of the mechanism to ensure consistency in the application of the General Data Protection Regulation throughout the EU;
- informing the Parliament, the Government, the European Commission, and the European Data Protection Board on its activities by means of an annual activity report.

In addition to the national authority, there is the European Data Protection Board (EDPB) acting at both the European and national levels. The EDPB is an independent European body. It is the umbrella organization which brings together the national data protection authorities (National Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS) for ensuring a consistent application and enforcement of data protection law across the EEA, and providing general guidance (including guidelines, recommendations and best practices).

www.peterkapartners.com/en/local/bucharest/

8.3 Role, functions and powers of civil/criminal courts in the field of data regulation

As per GDPR.

Specific Romanian regulations

If, in the exercise of its legal powers, the national supervisory authority considers that any of the rights of data subjects guaranteed by the legal regulations on the protection of personal data have been infringed, it may bring the matter before the competent court, in accordance with the law.

In this situation, the data subject shall automatically acquire the status of complainant and shall be summoned as such. If the data subject accepts the action, the National Supervisory Authority's capacity to bring proceedings shall cease. If the person concerned does not accept the action brought by the national supervisory authority, the court shall cancel the application in accordance with the Code of Civil Procedure.

Actions and applications, including those for ordinary or extraordinary legal remedies, brought by the National Supervisory Authority shall be exempt from the payment of stamp duty.

On the other hand, courts intervene directly when data protection crimes are being committed. Such crimes are: illegal access to a computer system, illegal interception of a computer data transmission, altering the integrity of computer data, disrupting the operation of computer systems, unauthorized transfer of computer data, and illegal operations with computer devices or software.

Consequences of non-compliance

As per GDPR.

Specific Romanian regulations

The violation of the following constitutes an infringement and is punishable by administrative fines of up to EUR 20,000,000 or, in the case of a company, up to 4% of the turnover:

- Processing of genetic data, biometric data or health data
- Processing of a national identification number
- Processing of personal data in the context of employment relationships
- Processing of personal data and special categories of personal data in the context of the performance of a task carried out in the public interest
- Processing of personal data for journalistic purposes or for purposes of academic, artistic, or literary expression
- Processing of personal data for scientific or historical research purposes, for statistical purposes, or for archiving purposes in the public interest

- Processing of personal data by political parties and organizations of citizens belonging to national minorities, non-governmental organizations

Conclusion

As can be observed throughout this guide, Romania focuses mainly on the GDPR for the protection of personal data, with additions being made by Law No. 190/2018 which regulates the situation of special categories of data, the authority in charge of data protection at the national level, and the way of sanctioning and the penalties applicable in case of non-compliance with the legal provisions applicable to data protection.

Contact Us

+40 21 310 48 82

www.peterkapartners.com/en/local/bucharest/

ciupala@peterkapartners.ro

33 Aviatorilor Boulevard,2nd floor, 1st District
Bucharest, 011853 Romania

Spain

López-Ibor DPM Abogados is a prestigious and internationally recognized full-service Spanish law firm with strategic offices in Madrid, Barcelona, and Valencia.

López-Ibor DPM Abogados has been recognized as a leading full-service firm by the most prestigious international rankings such as Chambers & Partners, Legal 500, IFLR100, World Tax, and Best Lawyers.

Our commitment to excellence is built on a foundation of extensive experience and a track record of success. With a legacy that extends over many years, our firm has consistently delivered unique solutions to a diverse range of legal challenges. What sets us apart is the unwavering loyalty and closeness demonstrated by our clients, reflecting the trust they place in our expertise.

At López-Ibor DPM Abogados, we offer comprehensive legal counsel across various domains, including Corporate and Commercial Law, Intellectual Property, Employment Law, Taxation, and New Technologies.

Our specialized New Technologies department focuses on safeguarding personal data, e-commerce, and social media. This encompasses professional support in crafting privacy policies, general terms of sale for online stores, and terms of use for websites. We also provide legal assistance in online contracting, commercial activities, advertising, Internet and social media, protection of intellectual property rights, and issues related to labor law in the realm of new technologies. Notably, we have successfully addressed cybercrimes committed by hackers through online interventions.

Furthermore, our expertise extends to data protection regulations, where we offer timely advice to ensure compliance with the General Data Protection Regulation (GDPR). We meticulously review companies' internal policies and procedures concerning data protection, aligning

https://lopez-iborabogados.com/en/

them with the latest Spanish and European regulations. Our thorough examination of contracts ensures the incorporation of clauses pertaining to data protection and confidentiality, tailored to the nature of each agreement.

At López-Ibor DPM Abogados, we pride ourselves on being at the forefront of legal innovation, providing steadfast support to our clients in navigating the complexities of contemporary legal landscapes.

Introduction

We have compiled the main differences between the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR") and the local Spanish Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights, mentioning only the differences where the Spanish legislation has added or modified some of the rights and provisions of the aforementioned European regulation.

In the following headings and subheadings, we will only address the points where there are noteworthy differences in the Spanish legislation with respect to the GDPR. We will not include any content in the headings and subheadings where there are no particularities in the Spanish legislation with respect to the GDPR.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The **Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights** (hereinafter, **"Spanish DP Law"**) is the Spanish national law that complements and develops the provisions of the GDPR and applies throughout the entire Spanish territory.

2.2. Additional or ancillary regulation, directives, or norms

Law 11/2023, of 8 May, introduced various amendments to the Spanish DP Law through its Second Final Provision. These include the replacement of the warning ("apercibimiento") as a sanction with a formal requirement, the regulation of investigative actions using digital systems, and the extension of the maximum duration of sanction procedures from nine to twelve months and of preliminary investigative proceedings from twelve to eighteen months. The reform also modifies the rules on substitution of the Presidency of the Spanish Data Protection Agency (AEPD) in cases of absence, vacancy, or recusal, to ensure continuity in the Agency's supervisory functions.

2.3. Upcoming or proposed legislation (if applicable)

While no formal legislative amendments to the Spanish DP Law are currently under parliamentary consideration, significant regulatory developments at the EU level are expected to affect the Spanish data protection framework. Most notably, the European Union Artificial Intelligence Act (AI Act) was adopted in 2024 and entered into force on 1 August 2024. Its provisions will become applicable gradually between 2025 and 2026.

The AI Act introduces obligations for AI systems that process personal data, including systems classified as high-risk or prohibited. It reinforces the application of GDPR principles – such as data minimization and data protection by design and by default – throughout the entire lifecycle of an AI system. As stated in Recital 69 of the AI Act, these obligations may include measures such as anonymisation, encryption, and the use of privacy-preserving technologies that allow algorithms to be trained without transmitting or copying raw data.

The Spanish Data Protection Agency (AEPD) is expected to play a key role in overseeing compliance with these provisions, particularly when AI systems involve the processing of personal data. As a result, future regulatory adjustments or guidance at the national level are likely to ensure full alignment between the AI Act and the Spanish DP Law.

Scope of Application

3.1. Legislative Scope

The Spanish DP Law applies within the territorial scope of Spain and governs processing activities carried out by entities established in Spain or, in certain cases, by entities not established in Spain when specific conditions under the GDPR or Spanish law are met. In contrast, the GDPR has a broader scope, applying across all EU Member States, and under Article 3(2), also to certain controllers or processors outside the EU that target individuals in the EU.

3.2 Statutory exemptions

While the GDPR outlines general exemptions in Article 2(2) and Article 23, the Spanish DP Law provides additional clarifications in certain contexts.

These include certain exemptions applicable to the use of video surveillance systems, which are regulated under Article 22 of Spanish DP Law. This provision allows the processing of images by public or private entities for security purposes and modulates the application of some GDPR obligations, such as the duty to inform data subjects (which may be fulfilled by visible signage). It also defines specific data retention periods and excludes domestic use of home cameras from the GDPR's scope when operated by individuals.

Additionally, Article 23 of the Spanish DP Law establishes systems of advertising exclusion, allowing the processing of data for the purpose of avoiding the sending of commercial communications to individuals who have exercised their right to object. These systems operate without requiring prior consent from the data subject, provided that their objection is respected, in accordance with Article 21 of the GDPR.

Furthermore, Article 23 of the GDPR permits Member States to restrict the scope of certain data subject rights when such limitations are necessary and proportionate to safeguard national security, criminal investigations, or other important public interests. The Spanish DP Law incorporates such limitations where appropriate under Spanish law.

3.3 Territorial and extra-territorial application

Article 3(2) of the GDPR establishes that controllers or processors not established in the European Union (EU) may still be subject to its provisions in certain circumstances. Specifically, the GDPR applies to the processing of personal data of individuals located in the EU where the processing is related to:

- the offering of goods or services to such data subjects in the EU, regardless of whether payment is required; or
- the monitoring of their behavior, insofar as that behavior takes place within the EU.

This means that entities located outside the EU

https://lopez-iborabogados.com/en/

—regardless of their location or nationality— must comply with the GDPR when they target individuals in the EU market. For example, a company based in the United States or China processing personal data of individuals residing in Spain would be subject to the GDPR under these conditions.

Although the Spanish DP Law does not have an extraterritorial effect, it complements the GDPR within Spanish jurisdiction. Furthermore, Article 70.1(c) of the Spanish DP Law confirms that representatives of controllers or processors not established in the EU are subject to the sanctioning regime under both the GDPR and the Spanish DP Law, when acting within Spanish territory or when designated as local representatives under Article 27 of the GDPR.

Legislative Framework

4.1. Key stakeholders

Data Protection Officer (DPO)

In Article 37, the GDPR broadly outlines the criteria and circumstances for the appointment of a Data Protection Officer ("DPO") within an organization. Conversely, the Spanish DP Law delves deeper by enumerating a specific list of organizations that are obliged to designate a DPO, surpassing the general guidelines provided by the GDPR. This expanded list —set out in Annex I of the Spanish DP Law— includes entities such as professional associations and their overarching councils, educational institutions,

In Article 37, the GDPR broadly outlines the criteria and circumstances for the appointment of a Data Protection Officer ("DPO") within an organization. Conversely, the Spanish DP Law delves deeper by enumerating a specific list of organizations that are obliged to designate a DPO, surpassing the general guidelines provided by the GDPR. This expanded list includes entities such as professional associations and their overarching councils, educational institutions, providers of information society services, as well as insurance and financial services entities, among others.

The Spanish DP Law, therefore, extends the scope of DPO requirements beyond the parameters established in the GDPR, outlining a more detailed and nuanced set of criteria applicable to specific sectors and contexts.

Records of processing activities

GDPR, in its article 30, stipulates that *"Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility", however, it would not apply to "an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data".*

The legal framework in Spain, as articulated in the Spanish DP Law, introduces an additional requirement for certain organizations or entities. According to this provision, such entities —primarily public authorities or bodies— are obliged to publicly disclose and publish a comprehensive inventory of their data processing activities. This disclosure must be easily accessible through electronic means, encompassing all the details specified in Article 30 of the GDPR. In essence, the Spanish DP Law extends beyond the GDPR by specifically stipulating the obligation for certain entities to proactively share and maintain a transparent record of their data processing endeavors, thereby fostering greater accountability and accessibility.

Usually, these organizations will be public or administrative.

Among the organizations listed, we can mention:

- Courts of Justice
- The National Bank of Spain ("Banco de España")
- Public universities
- Parliamentary groups
- Public bodies and public law entities.
- State Administration

Requirements for Data Processing

5.1. Data storage and retention timelines

Under Article 5(1)(e) of the GDPR, personal data must be retained only for as long as necessary for the purposes for which they were collected. Once that period ends, data should be deleted or anonymized, unless continued retention is legally justified.

The Spanish DP Law introduces an additional requirement known as the "blocking" obligation, set out in Article 32 of the Spanish DP Law. When data are no longer necessary for their original purpose but must be retained to comply with legal obligations (such as for liability or audit purposes), they must not be deleted immediately but blocked; that is, stored in a way that restricts their processing and access exclusively for those legal purposes.

During the blocking period, the data cannot be used for any other purpose and must be securely retained until final deletion becomes possible.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

- *Right to grievance redressal and appeal*

In addition to the remedies provided under Articles 77 to 79 of the GDPR, the Spanish DP Law establishes a detailed administrative procedure for the protection of data subjects' rights before the Spanish Data Protection Agency (AEPD).

Articles 63 to 69 of the Spanish DP Law regulate the lodging and processing of complaints, including mechanisms for resolving them through a simplified procedure introduced by Law 11/2023. The AEPD may initiate investigations, issue warnings or sanctions, and require corrective measures. The law sets a maximum deadline of twelve months for resolving complaints, starting from their admission for processing.

Processing of Children or Minors' data

The GDPR establishes that the processing of personal data of a child in relation to information society services is only lawful when the child is at least 16 years old, unless a Member State sets a lower age threshold, which may not be below 13 years.

In Spain, Article 7 of the Spanish DP Law (LOPDGDD) sets this threshold at **14 years of age.** Therefore, children aged 14 or older may provide valid consent for the processing of their personal data in the context of information society services.

However, an important exception applies: if the act or legal transaction the child wishes to carry out requires parental or guardian authorization, then the consent for data processing must also be granted by the parents or legal representatives, regardless of the child's age.

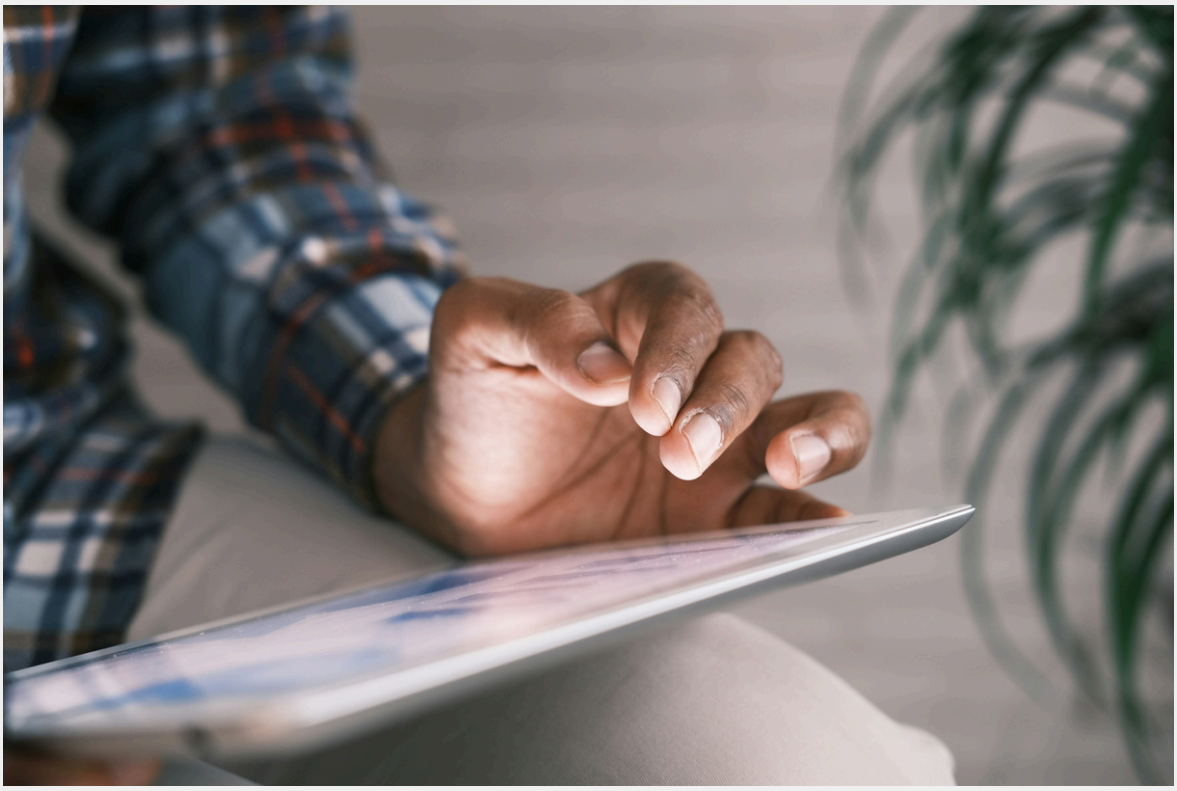
A typical example would be online purchases, which usually fall within this category of acts requiring legal capacity and parental authorization under Spanish civil law.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

Each Member State is obliged to create its own internal authority to oversee data protection in the country.

Under article 44 of the **Spanish DP Law, the Spanish Data Protection Agency** ("Agencia Española de Protección de Datos", "**AEPD**") is the statutory authority with jurisdiction in data protection matters in the country.



AEPD stands as an independent administrative authority with nationwide jurisdiction, as outlined in Law 40/2015, dated October 1, which governs the Legal Regime of the Public Sector. The AEPD has legal personality and enjoys both public and private capacities, operates autonomously, and is independent from other public authorities in the execution of its duties. Its formal link with the government is established through the Ministry of Justice. Additionally, the AEPD assumes the role of representative of all the data protection authorities within the Kingdom of Spain in front of the European Data Protection Committee.

8.2. Role, functions, and powers of authorities (if applicable)

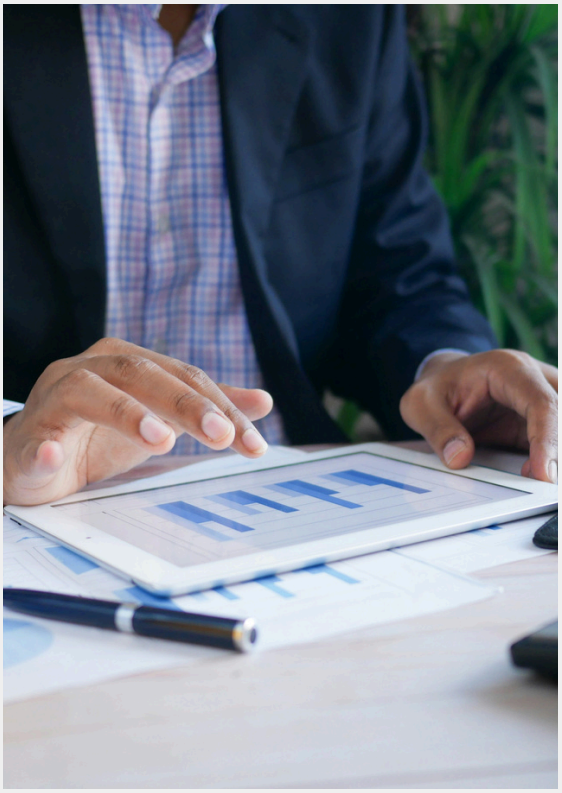
One of the primary responsibilities of the AEPD is to oversee the application of both the Spanish DP Law and the GDPR. Specifically, it is tasked with executing the functions described under Article 57 and wielding the powers listed under Article 58 of the GDPR, as well as those stipulated in the Spanish DP Law and its associated implementing provisions.

Furthermore, the AEPD assumes the duty of carrying out functions and exercising powers delegated to it by other laws or regulations within the framework of European Union Law. This multifaceted role underscores the AEPD's pivotal position in upholding data protection standards, both nationally and within the broader European context.

- Role, functions, and powers of additional or ancillary data regulation authorities (if applicable).

As of today, there are three regional data regulation authorities: the Catalan Data Protection Authority, the Basque Data Protection Agency, and the Council for Transparency and Data Protection of Andalusia. The latter was created in 2014, with the special feature that in this region ("Comunidad Autónoma"), the competent entity in data protection matters is also competent in transparency matters.

Each one of them has particular functions for their own regions,



which mainly involves monitoring the application of the data protection regulation in their territory and specially when entities of the public sector of those regions are involved in the data processing.

Nevertheless, the AEPD continues to serve as the overseeing authority across the entire territory, encompassing the three aforementioned regions with which it collaborates and enforces mechanisms for coherence.

8.3. Role, functions, and powers of civil/criminal courts in the field of data regulation

The contentious-Administrative Sections of the Central Court of First Instance ("Secciones de lo Contencioso-Administrativo del Tribunal Central de Instancia") are responsible for authorizing, by means of an order, the requests for information issued by the AEPD and other independent administrative authorities at the state level to operators providing publicly available electronic communications services and providers of information society services, when this is necessary in accordance with the Spanish DP Law.

Moreover, the Contentious-Administrative Section of the Supreme Court will decide on the request for authorization for the declaration provided for in the Fifth Additional Provision of the Spanish DP Law, when such a request is made by the General Council of the Judiciary ("Consejo General del Poder Judicial").

Such Fifth Additional Provision of the Spanish DP Law refers to the judicial authorization in relation to decisions of the European Commission on international transfer of data.

Finally, the Contentious-Administrative Section of the National Audience ("Audiencia Nacional") will also decide on the request for authorization for the declaration provided for in the Fifth Additional Provision of the Spanish DP Law, when such a request is made by the AEPD.

Consequences of non-compliance

9.1. Consequences and penalties for data breach

Sanctions and penalties under the General Data Protection Regulation (GDPR) and the Spanish DP Law share foundational principles but exhibit nuanced distinctions. Within the overarching framework, both regulations empower regulatory authorities to impose fines for breaches, yet their specific applications diverge to some extent.

In the broader spectrum, the GDPR provides a comprehensive foundation for penalties, delineating a general framework that allows for substantial fines as a response to infringements.

https://lopez-iborabogados.com/en/

The maximum penalty, levied for severe violations, can reach up to 4% of the global annual turnover or EUR 20,000,000.-, depending on which amount is greater. This regulation incorporates a flexible approach, recognizing the varied nature and seriousness of potential violations.

Conversely, the Spanish DP Law maintains a parallel structure while introducing specific provisions tailored to the Spanish legal context. Although aligned with the GDPR's fundamental core principles, it establishes distinct rules regarding the imposition of penalties within the Spanish territory, including the determination of specific fine amounts. These reflect Spain's commitment to effectively addressing data protection breaches at the national level."

While the GDPR lays out general criteria for imposing fines —taking into account factors such as the nature, severity, and duration of the violation— the Spanish DP Law adapts these criteria to ensure consistency with the Spanish legal system. It provides a mechanism for authorities to assess breaches in light of the specific circumstances that may arise within Spain's regulatory framework. For instance, Spanish DP Law establishes a statute of limitations for penalties depending on the amount of the fine, with limitation periods ranging from one (1) to three (3) years."

Therefore, while the fundamental concept of imposing penalties for data protection breaches remains consistent throughout the GDPR, the Spanish DP Law contains particularities to ensure an effective, contextually relevant application of sanctions within its jurisdiction.

9.2. Consequences and penalties for other violations and non-compliance

Conclusion

In conclusion, the examination of the Spanish DP Law in contrast to the General Data Protection Regulation (GDPR) has revealed several distinctive features that underscore the specific approach and nuanced framework established by Spanish legislation. Below is a summary of the most significant differences:

A. Different Age of Consent:
Spanish DP Law has introduced a distinctive age threshold for the valid consent of minors, setting it at the age of 14 years. This deviation from the GDPR's uniform age requirement reflects Spain's emphasis on tailoring regulations to specific cultural and social contexts.

B. Designation of a Data Protection Officer (DPO) for Public Authorities:
Spanish regulations uniquely mandate the appointment of a DPO for all public authorities and entities, regardless of their size. This proactive measure reflects a commitment to enhancing accountability and compliance within the public sector.

C. Sanctioning Authority:
In Spain, the AEPD assumes a central role as the primary authority responsible for imposing sanctions for data protection infringements. This centralized structure contrasts with the more decentralized model under the GDPR, where different supervisory authorities in each EU Member State are empowered to impose sanctions independently.

These distinctions emphasize the importance of thoroughly understanding the specific characteristics of the Spanish data protection framework. As businesses and organizations navigate the complexities of compliance, being aware of these unique features is essential to ensure full adherence to both the Spanish DP law and the broader GDPR.

LÓPEZ-IBOR DPM ABOGADOS

Should you wish to expand on the content of this article or seek guidance on the Spanish Data Protection regulations, our team would be delighted to assist you. You are welcome to contact us at your convenience.

Jaime Morey:
jaime.morey@l-ia.com

Pablo Stöger:
pablo.stoger@l-ia.com

Alfonso López-Ibor:
alfonso.lopezibor@l-ia.com

Arianna Vergani:
arianna.vergani@l-ia.com

Contact Us

+34 91 52 17 818

www.lopez-iborabogados.com

jaime.morey@l-ia.com

Calle López de Hoyos, 35, 3º
E-28002 Madrid (Spain)

Ukraine

PETERKA & PARTNERS is a full-service law firm operating in Central and Eastern Europe, providing one-stop access as an integrated regional service. The firm provides legal services to multinational companies active in the region, as well as leading local groups, providing them with complex legal solutions with exceptional commercial value.

Introduction

Below is a brief outline of the legal regulation of personal data protection in Ukraine.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The main legal act governing data protection in Ukraine is the Law of Ukraine on Personal Data Protection No. 2297-VI dated 1 June 2010, as amended (the **"PDP Law"**).

2.2. Additional or ancillary regulation, directives, or norms

Apart from the PDP Law, the main additional regulations for data protection are established by the legal acts adopted by the Ukrainian Parliament Commissioner for Human Rights (the **"Commissioner"**), such as the Model Procedure on Processing of Personal Data; the Procedure on Notification of the Commissioner on the Processing of Personal Data that Constitutes a Special Risk for the Rights and Freedoms of Personal Data Subjects, On the Structural Unit or Responsible Person that Organises the Work related to Protection of Personal Data during its Processing and the Publication of Such Information (the **"Procedure on Special Risk Data"**); others.

2.3. Upcoming or proposed legislation

Since Ukraine is on track to join the European Union, it has to ensure the protection of personal data in accordance with the highest European and international standards. In that respect, Ukraine is constantly working on draft laws aimed at harmonising current legislation on data protection, particularly with the standards provided for by the General Data Protection Regulation (Regulation (EU) 2016/679). Currently, no draft law in this respect has yet been adopted.

Scope of Application

3.1. Legislative Scope

3.1.1. Definition of personal data

The PDP Law defines "personal data"

Contact Us

+380 44 581 11 20

https://www.peterkapartners.com/en/local/kyiv/

utiralov@peterkapartners.ua

45/85 Saksahanskoho St.
Kyiv, 01033 Ukraine

as information or a set of information on a natural person who is, or may be, explicitly identified.

3.1.2. Definition of different categories of personal data

The PDP Law contains special requirements for processing certain personal data that constitutes a special risk to the rights and freedoms of data subjects ("Special Risk Data").

Under the PDP Law, the Special Risk Data includes personal data on racial or ethnic origin, political, religious or philosophical beliefs, membership in political parties and trade unions, criminal convictions, health, sex life, biometric, and genetic data.

The Procedure on Special Risk Data expands the list of Special Risk Data provided by the PDP Law and includes personal data about national origin, membership in political organisations, religious organisations or public organisations with an ideological orientation, being brought to administrative or criminal liability, application of measures to a person within the framework of a pre-trial investigation, the taking of measures against a person provided for by the Law of Ukraine on Operative Investigation Activity, committing certain types of violence against a person, location and/or routes of movement of the person.

3.1.3. Treatment of data and its different categories

Personal data processing is defined under the PDP Law as any operation or set of operations, such as collection, recording, accumulation, storage, adaptation, alteration, renewal, use and distribution (dissemination, realisation, transmission), depersonalisation, destruction of personal data, including with the use of information (automated) systems.

Personal data must be accurate, reliable, and updated as necessary for its processing. The composition and content of personal data must be appropriate, adequate, and not excessive in relation to the purpose of its processing.

The processing of personal data is carried out for specific and lawful purposes, determined by the consent of the personal data subject or in cases provided for by the laws of Ukraine, in the manner established by the legislation. It is not allowed to process the personal data of a natural person without his/her consent if such data is confidential information, except for those cases determined by law, and only in the interests of national security, economic welfare, and human rights.

The procedures for processing, the timeline of processing, and the composition of personal data must be proportional to the purpose of processing. The purpose of personal data processing must be explicit,

legitimate and determined before collection begins. If a specific purpose for personal data processing is changed to a new purpose that is incompatible with the previous one, for further data processing, the data controller, except in cases specified by law, must obtain the consent of the data subject to process the data in accordance with the new purpose.

As to the Special Risk Data, its processing is allowed only if unambiguous consent has been given by the data subject or based on exemptions envisaged by the PDP Law (e.g., for employment and healthcare purposes, protection of the vital interest of the data subject, law enforcement intelligence or counterintelligence activity, anti-terrorism). Under the general rule, the data controller must notify the Commissioner of processing Special Risk Data within 30 business days from the start of such processing. There is also an obligation to notify the Commissioner in cases of the alteration of Special Risk Data or termination of its processing.

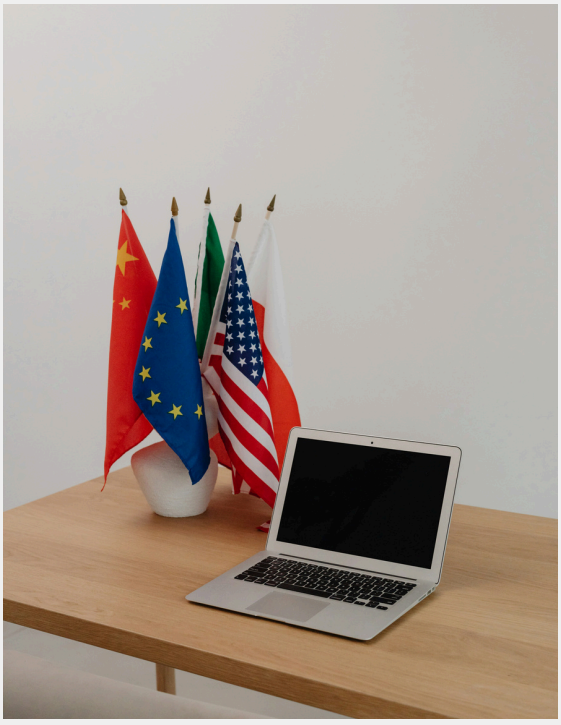
3.2. Statutory exemptions

The processing of personal data is allowed without adherence to the provisions of the PDP Law if such processing is made: (a) by a natural person purely for personal or household needs; (b) exclusively for journalistic and creative purposes, given a balance is ensured between the right to respect the private life and the right of freedom of expression. The PDP Law also does not cover relations on the receipt of archival information from repressive bodies.

In specific cases, i.e., in cases provided by law to the extent required in a democratic society in the interests of national security, economic welfare, or protection of the rights and freedoms of data subjects or other persons, certain provisions of the PDP Law may be limited.

3.3. Territorial and extra-territorial application

The PDP Law does not specify the territory of its application. However, according to the general principles of Ukrainian law and practice, it may be interpreted to apply to all personal data processed in the territory of Ukraine.



https://www.peterkapartners.com/en/local/kyiv/

Legislative Framework

4.1. Key stakeholders

- "Data Controller" is a natural person or legal entity who determines the purpose of personal data processing, the composition of this data, and the procedures for its processing unless otherwise specified by law.

- "Data Processor" is a natural person or legal entity who is granted the right by the data controller or by law to process this data on behalf of the data controller.

- "Data Subject" is a natural person whose personal data is processed.

4.2. Role and responsibilities of key stakeholders

The data controller and processor solely determine the procedure for processing personal data, taking into account the specifics of the processing of personal data in various areas.

In particular, the data controller determines the:

- purpose and grounds for processing personal data;
- categories of data subjects;
- composition of personal data;
- procedure for processing personal data, namely the:
  - method of collection and accumulation of personal data;
  - timeline and conditions for storage of personal data;
  - conditions and procedure for alteration, deletion or destruction of personal data;
  - conditions and procedure for the transfer of personal data and a list of third parties to whom personal data may be transferred;
  - procedure for access to the personal data of the persons carrying out the processing, as well as to the data subjects;
  - measures to ensure personal data protection;
  - procedure for storage of information on operations related to the processing of personal data and access to them;
  - obligations and rights of persons responsible for organising work related to personal data protection during its processing.

The data controller may entrust the personal data processing to the data processor under a written agreement. The data processor may process personal data only for the purposes and to the extent specified in such agreement.

Requirements for Data Processing

5.1. Grounds for collection and processing

-Consent
The consent of the data subject is the voluntary expression of the will of

https://www.peterkapartners.com/en/local/kyiv/

a natural person (subject to his/her awareness) to grant permission to process his/her personal data in accordance with the stated purpose of its processing, expressed in written form or in a form that makes it possible to conclude that consent has been granted.

The consent may be prepared as a separate document to be signed by the data subject, or a corresponding indication in electronic form, a term and condition of the agreement, or it may be prepared in any other form that allows the conclusion that consent has been provided (writing an application, filling in a questionnaire, etc.).

In the field of electronic commerce, the data subject's consent may be provided when registering in the information and communication system of the electronic commerce subject by ticking the granting of permission to process his/her personal data in accordance with the stated purpose of its processing, provided that such a system does not create opportunities for personal data processing until the tick is made.

As a general rule, at the time of collection of personal data, the data subject shall be informed about the data controller, composition and content of collected personal data, the data subject's rights defined by the PDP Law, the purpose of collecting personal data, and the persons to whom the relevant personal data may be transferred

-Consent Notice

The consent notice should be in a simple and understandable form and contain the full scope of information that must be provided by the data controller to the data subject before receipt of the consent.

-Withdrawal of Consent

The data subject has the right to withdraw consent to processing personal data without specifying motives if the only basis for processing is his/her consent. From the moment of withdrawal of consent, the data controller is obliged to stop personal data processing.

-Other grounds prescribed by law

Apart from the consent, the PDP Law establishes a list of other grounds allowing the processing of personal data without the consent of the data subject (such as the conclusion and performance of a transaction to which the data subject is a party or which is concluded in favour of the data subject or for the implementation of measures preceding the conclusion of the transaction at the request of the data subject, etc.).

5.2. Data storage and retention timelines

The personal data is processed no longer than necessary for the legitimate purposes for which it was collected or further processed; in any case, no longer than provided for by the legislation in the field of archival affairs and record keeping. Further processing of personal data for

historical, statistical, or scientific purposes may be carried out subject to ensuring its proper protection.

5.3. Data correction, completion, updation, or erasure of data

The personal data shall be changed based on a substantiated written request of the data subject or in other cases prescribed by law (e.g., upon a court decision that has entered into force). If information about a person is found to be untrue, such information must be immediately changed or destroyed. Personal data shall be updated if necessary, determined by the purpose of its processing.

Personal data shall be deleted or destroyed in the case of:

- expiration of the data storage period determined by the consent of the data subject or by law;
- termination of the legal relationship between the data subject and controller or processor, unless otherwise provided for by law;
- issuance of an appropriate order of the Commissioner or officials of its secretariat;
- entry into force of a court decision on personal data deletion or destruction;
- personal data collected in violation of the requirements of the PDP Law

5.4. Data protection and security practices and procedures

The data controllers, processors and

https://www.peterkapartners.com/en/local/kyiv/

third parties are obliged to ensure personal data protection from accidental loss or destruction, and from illegal processing, including illegal destruction or access to personal data. The data controllers and processors take measures to maintain the security of personal data in all stages of their processing, including organisational and technical measures. They independently determine the list and composition of security measures, taking into account the requirements of the legislation and informational security.

The organisational measures include:

- establishment of a data access procedure for employees of data controllers/processors;
- establishment of the procedure for recording operations related to personal data processing and access to them;
- elaboration of an action plan in case of unauthorised access to personal data, damage to technical equipment, or emergencies;
- regular training of employees working with personal data.

Technical security measures are taken, in particular, to exclude unauthorised access to personal data and ensure the proper working of the technical and program means through which the personal data is processed.

Data controllers and processors processing Special Risk Data are obliged to (1) create/define a structural unit or responsible person for organising the work related to personal data protection during its processing and (2) notify the Commissioner about such unit/person.

5.5 Disclosure, sharing, and transfer of data

Sharing of personal data is allowed according to the data subject's consent or in cases specified by law and only (if required) in the interests of national security, economic welfare, human right,s and for conducting the all-Ukrainian population census.

The data controller shall notify the data subject of the personal data transfer to a third party within ten working days if required by the conditions of his/her consent or otherwise not provided for by law. The specified notifications are not made in the case of:

- transfer of personal data upon requests made within the performance of the tasks of law enforcement, intelligence, or counterintelligence, anti-terrorism activities;
- exercise by state and local authorities of their powers provided for by law;
- personal data processing for historical, statistical, or scientific purposes;

https://www.peterkapartners.com/en/local/kyiv/

- notification of the data subject on such transfer while collecting personal data in accordance with the PDP Law.

5.6. Cross-border transfer of data

The transfer of personal data to foreign subjects is carried out only if the relevant state ensures adequate personal data protection. The following states are recognised as doing so: (i) European Economic Area (EEA) member states; (ii) states-signatories to the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data of 28.01.1981; and (iii) other states defined as such by the Cabinet of the Ministers of Ukraine.

Additionally, cross-border transfer of personal data is allowed if the:

- data subject grants unambiguous consent to the transfer;
- need exists to conclude or perform an agreement between the data controller and the data subject for the benefit of the data subject;
- need exists to protect the vital interests of the data subject;
- need exists to protect public interest, establish, implement, and ensure the legal claim;
- data controller has provided relevant guarantees of non-interference in the personal and family life of the data subject.

Personal data may not be shared with a purpose other than the one for which it was collected.

https://www.peterkapartners.com/en/local/kyiv/

5.7. Grievance redressal

Data subjects can submit complaints regarding their personal data processing to the Commissioner or a court.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

-Right to withdraw consent

Please see the related information in para 5.1. above.

-Right to grievance redressal and appeal

Please see the related information in para 5.7. above.

-Right to access information

In particular, the data subject has the right to (i) access to his/her personal data; (ii) no later than 30 calendar days from the date of receipt of the request, except in cases provided for by law, and receive a response on whether his/her personal data is being processed, as well as receive the content of such personal data; (iii) know about the sources of collection, location of his/her personal data, the purpose of their processing, location or place of residence of the data controller and processor, or authorise persons to receive such information, except in cases established by law; (iv) receive information on the conditions for

granting access to personal data, in particular, information on third parties to whom his/her personal data is transferred; (v) know the mechanism for automatic personal data processing.

-Right to nominate

The PDP Law does not explicitly provide for the right to nominate.

6.2. Duties

The PDP Law does not set out specific duties for data subjects, except for implicit general ones such as an obligation to comply with personal data protection legislation.

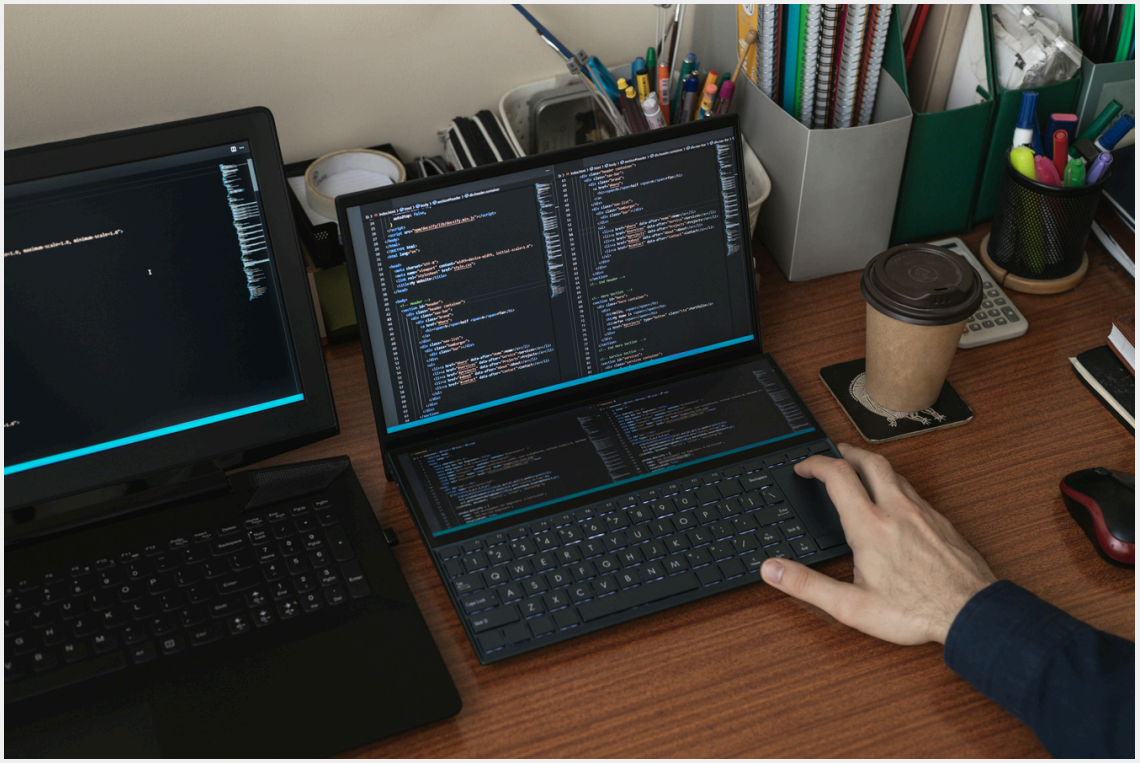
Processing of Children or Minors' data

The PDP Law does not regulate the processing of the data of children or minors. Under general civil law, parents or guardians may act on their behalf, including providing the consent required for personal data processing.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

According to the PDP Law, the Commissioner and courts are



https://www.peterkapartners.com/en/local/kyiv/

responsible for checking for compliance with personal data protection legislation.

8.1. Overview of relevant statutory authorities

According to the PDP Law, the Commissioner and courts are responsible for checking for compliance with personal data protection legislation.

8.2. Role, functions, and powers of authorities

The key powers of the Commissioner are the following:

- to receive and decide on proposals, complaints, and other requests from natural persons and legal entities related to personal data protection;
- to conduct inspections of data controllers or processors;
- to issue binding demands (instructions) on the prevention or elimination of violations of personal data protection legislation, to draw up protocols on bringing one to administrative liability and sending them to the court in cases provided for by the law;
- to approve regulations in the field of personal data protection;
- to provide recommendations on the practical application of personal data protection legislation, to clarify the rights and obligations of the relevant persons, and to provide, at the respective request, opinions on draft codes of conduct in the field of personal data protection;
- to propose amendments to legislation on personal data protection, to monitor new practices, tendencies and technologies regarding personal data protection, etc.

8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

In respect of being brought to liability, civil courts consider and decide on protocols for bringing one to administrative liability, submitted by the Commissioner or officials of its Secretariat. Criminal courts consider and decide on cases related to being brought to criminal liability for committed criminal offences.

Apart from the above, the courts also protect the rights of relevant participants in data protection relations. In particular, the data subjects may file lawsuits to the courts related to a breach of personal data protection legislation and recover compensation for damage, including moral damage, caused by such a breach.

Consequences of non-compliance

The following violations can be subject to administrative liability in the sphere of personal data protection:

- for failure to notify or late notification of the Commissioner on the processing of Special Risk

https://www.peterkapartners.com/en/local/kyiv/

- for failure to notify or late notification of the Commissioner on the processing of Special Risk Data, or amendments to such data, and the provision of incomplete or unreliable information, a fine of up to approximately EUR 140 is envisaged

- for failure to execute demands (instructions) of the Commissioner or officials of its Secretariat on the prevention or elimination of violations of personal data legislation, a fine of up to approximately EUR 350 is envisaged

- for non-compliance with personal data legislation resulting in unauthorised access to personal data or violation of the rights of a data subject, a fine of up to approximately EUR 350 is envisaged

- For repeated (within a year) of the above violations, a fine of up to approximately EUR 700 may be imposed.

Certain violations may also involve criminal liability. In particular, for the illegal collection, storage, use, destruction, or distribution of confidential information on a natural person or an illegal alteration of such information, a fine of up to approximately EUR 350 is envisaged or correctional works of up to two years, arrest of up to six months, or restraint of liberty of up to three years. For the same actions committed repeatedly, or in cases where they have caused substantial harm to the person's rights, freedoms, and interests, arrest of up to six months, restraint of liberty of up to five years, or imprisonment for the same term is envisaged.

Conclusion

Currently, it may not be concluded that Ukrainian legislation fully ensures personal data protection in compliance with the best international standards and practices in this area. However, Ukraine is constantly working on the harmonisation of its legislation with European and other international standards.

***

The above information is provided for general understanding and informational purposes only.

In general, this information is provided according to the standard legislation of Ukraine and does not focus on specific regulations that may, from time to time, be introduced into the legislation of Ukraine due to the martial law introduced in Ukraine since February 24, 2022, in response to the military aggression of the Russian Federation against Ukraine.

On no account can the provided information be considered as either a legal opinion or advice on how to proceed in particular cases or on how to assess them.

The protection of personal data may also involve other legal aspects. We strongly advise that legal advisors be involved in order to ensure that each specific case is dealt with comprehensively. Should you need any further information on the issues covered by this overview, please contact Mr. Taras Utiralov (utiralov@peterkapartners.ua) or Ms. Halyna Melnyk (melnyk@peterkapartners.ua).

Contact Us

+380 44 581 11 20

https://www.peterkapartners.com/en/local/kyiv/

utiralov@peterkapartners.ua

45/85 Saksahanskoho St.
Kyiv, 01033 Ukraine

United Kingdom

Introduction

1.1. Note: The UK has three separate legal jurisdictions: England & Wales, Scotland, and Northern Ireland. The laws set out apply to the whole of the UK, but enforcement may vary by jurisdiction. Fladgate advises on the law applicable to England & Wales.

1.2. The UK operates a comprehensive, GDPR-derived privacy regime anchored in the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018"), supplemented by the Privacy and Electronic Communications Regulations ("PECR"). Post-Brexit, the UK has retained a framework substantively aligned with the EU GDPR, while introducing UK-specific instruments for international transfers and distinct policy guidance, notably in children's data. The Information Commissioner's Office ("ICO") supervises compliance, issues guidance, and enforces across UK GDPR, DPA 2018, and PECR.

Contact Us

+44 20 3036 7000

https://www.fladgate.com/

epowell@fladgate.com

16 Great Queen Street
London, WC2B 5DG England

Governing Data Protection Legislation

2.1. Overview of principal legislation

2.1.1. UK GDPR is the primary instrument regulating the processing of personal data in the UK, preserving the principles, rights, and accountability architecture of the EU GDPR.

2.1.2. DPA 2018 supplements UK GDPR, including discrete parts for law enforcement processing (Part 3) and intelligence services (Part 4), and contains significant procedural, investigatory, and enforcement provisions.

2.1.3. PECR (which originally enacted EU Directive 2002/58/EC) governs direct marketing, cookies and similar technologies, traffic and location data, and confidentiality of communications.

2.1.4. Common law concepts of confidentiality and the right to privacy, and the Human Rights Act 1998 (incorporating Article 8 ECHR—respect for private and family life) complement statutory privacy protections in specific contexts.

2.2. Additional or ancillary regulation, directives, or norms

2.2.1. The Data Protection (Charges and Information) Regulations 2018 require all UK data controllers to register and pay a fee to the ICO.

2.2.2. The ICO has issued a number of statutory Codes of Practice, which are relevant for assessing compliance with UK GDPR. These codes include:

2.2.2.1. Data Sharing Code of Practice: A statutory code that provides practical guidance for organisations on sharing personal data in a way that complies with data protection law, aiming to give confidence to share data fairly and proportionately.

2.2.2.2. Age Appropriate Design Code of Practice: Aims to ensure that online services appropriately safeguard children's personal data by setting out standards for data protection and privacy by design.

2.2.2.3. Employment Practices Code: Provides guidance for employers on how to handle personal information about their employees in a way that respects their privacy while meeting the legitimate needs of the business.

2.2.2.4. Data Protection and Journalism Code Of Practice: Provides guidance for organisations that process personal data for journalism.

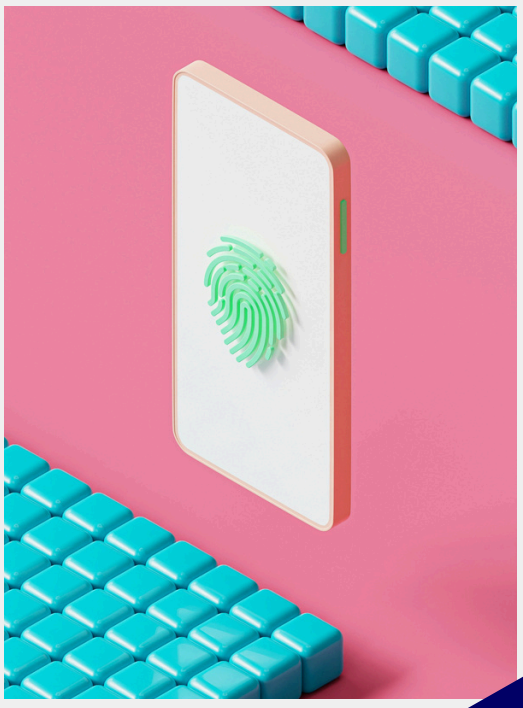
2.2.3. Sector-specific regimes influence privacy obligations in practice, including financial services expectations (FCA/PRA), health and NHS information governance, employment law, and cybersecurity frameworks.

2.2.4. The National Cyber Security Centre provides widely adopted security guidance.

2.2.5. For international transfers of personal data, the UK has the International Data Transfer Agreement ("IDTA") and the UK Addendum to the EU Standard Contractual Clauses ("SCCs"), together with transfer risk assessment expectations.

2.3. Upcoming or proposed legislation

2.3.1. The Data (Use and Access) Act 2025 was passed in 2025 and is being implemented in stages. This Act amends UK GDPR, DPA 2018, and PECR, with measures intended to streamline documentation and accountability, adjust cookies/consent expectations, and clarify uses of legitimate interests.



2.3.2. The EU's 2021 adequacy decision for the UK has a review date of late 2025; at the time of writing, the EU has proposed renewing the adequacy decision for a further 6 years.

Scope of Application

3.1. Legislative scope

The scope of the UK GDPR is in all material respects identical to that of the EU GDPR.

3.1.1. **Personal data** is defined (Art 1 UK GDPR) as information relating to an identified or identifiable living natural person, including indirect identifiers, when combined with other information reasonably likely to be used. No distinction is drawn between data held manually or electronically, or between personal data on consumers and personal data relating to commercial activity.

3.1.2. **Special category data** is defined (Art 9 UK GDPR) to include personal data relating to health, biometric identifiers used for identification, genetic data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. Data relating to criminal convictions is treated in the same way as special category data.

3.1.3. Art 5 UK GDPR sets out seven key principles regarding processing of personal data, and these are expanded in detailed provisions detailed below:

3.1.3.1. Lawfulness, fairness and transparency
3.1.3.2 Purpose limitation
3.1.3.3 Data minimisation
3.1.3.4 Accuracy
3.1.3.5 Storage limitation
3.1.3.6 Integrity and confidentiality (security)
3.1.3.7 Accountability

3.1.4. One key definition pertaining to personal data and its processing:

Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art 5 UK GDPR).

3.2. Exemptions

3.2.1. Processing for domestic purposes (personal or household activity) falls outside the scope of UK GDPR.
3.2.2. Limited exemptions exist for journalistic, academic, artistic, and literary purposes under balancing tests.
3.2.3. Separate regimes govern law enforcement and national security processing.
3.2.4. Specific exemptions restrict transparency and rights of the data subject where necessary (e.g., regulatory functions, legal privilege, management forecasts, negotiations).

3.3. Territorial and extra-territorial application

3.3.1. UK GDPR applies to:

3.3.1.1. controllers and processors established in the UK; and

3.3.1.1. controllers and processors outside the UK who offer goods or services to individuals in the UK or monitor the behaviour of those individuals (Art 3 UK GDPR).

3.3.2. PECR has no specific territorial provisions, but in practice, if electronic marketing uses personal data, use in breach of PECR is likely to also breach UK GDPR, and be caught by the principles set out in 3.3.1.

Legislative Framework

4.1. Key stakeholders

4.1.1. **Data Controller:** The organisation or individual that determines the purposes and means of processing personal data, and bears primary accountability for compliance, including selecting lawful bases, upholding rights, and ensuring processors are appropriately engaged and supervised.

4.1.2. **Data Processor:** A separate organisation that processes personal data on behalf of a controller under documented instructions. Processors must implement appropriate security, assist the controller with rights and DPIAs, maintain records, and permit audits; they may be directly liable for certain infringements.

4.1.3. **Joint Controllers:** Two or more controllers that jointly determine purposes and means of processing must transparently allocate responsibilities via an arrangement and make the main points available to data subjects.

4.1.4. **Data Subject:** The identified or identifiable individual to whom personal data relates. Data subjects benefit from a suite of rights and safeguards intended to provide transparency and control over their personal data.

4.1.5. **UK Representative (where required):** A locally designated UK contact for controllers or processors not established in the UK but caught by the UK GDPR due to offering goods or services to, or monitoring the behaviour of, individuals in the UK. The representative facilitates communication with data subjects and the ICO.

4.1.6. **Information Commissioner's Office (ICO):** The independent supervisory authority responsible for guidance, supervision, investigations, corrective orders and administrative fines under UK GDPR, and for approving codes of conduct and certification schemes.

4.1.7. **Data Protection Officer (DPO):** A role required in specified circumstances (e.g., public authorities or bodies; organisations whose core activities involve large-scale monitoring or large-scale processing of special category or

criminal offence data). The DPO acts independently of the controller, advises on compliance, monitors internal practices, and serves as a contact point for the ICO.

4.2. *Role and responsibilities of key stakeholders*

4.2.1. Controllers are primarily responsible for the processing of personal data that they control. Amongst their duties, they should:

4.2.1.1. implement appropriate technical and organisational measures for security;

4.2.1.2. establish a lawful basis for all processing activities,

4.2.1.3. ensure that any international data transfers comply with Chapter V UK GDPR;

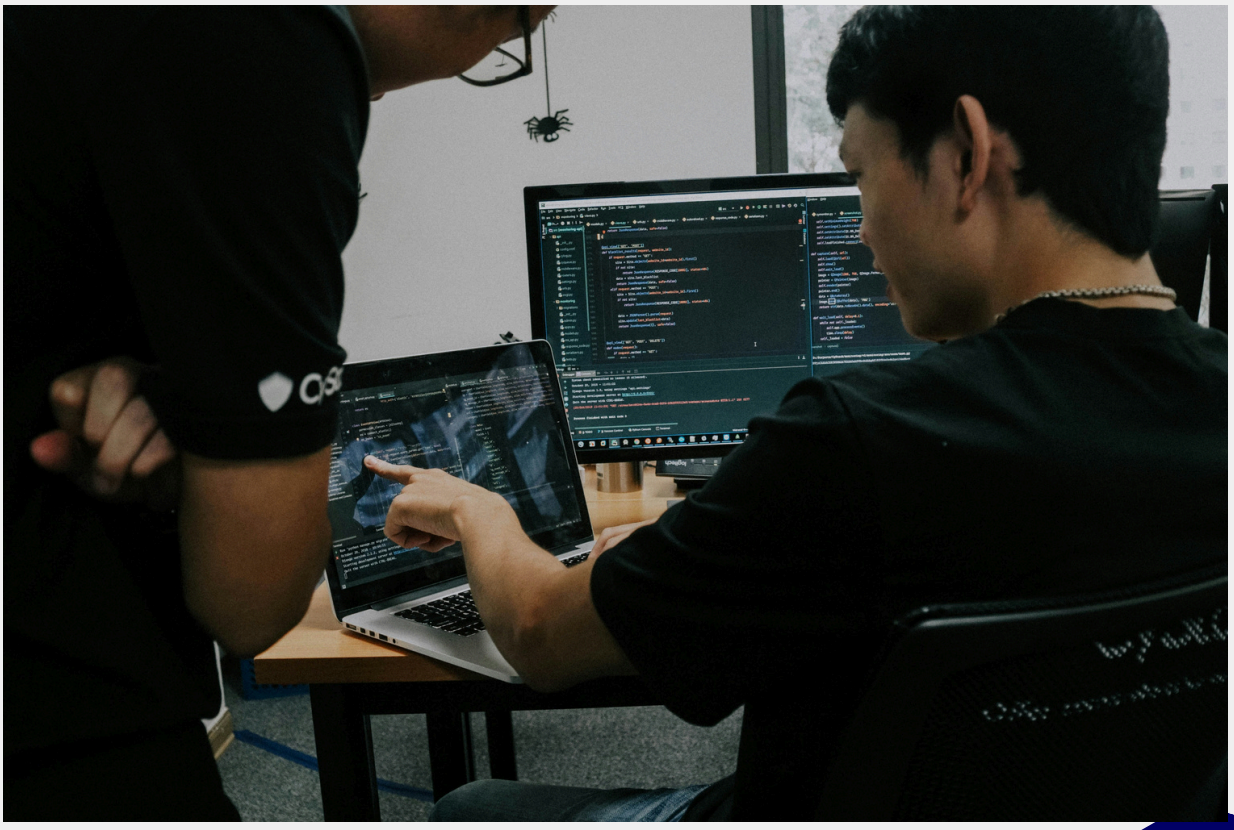
4.2.1.4. ensure data subjects' rights are respected, and any request to exercise is fulfilled;

4.2.1.5. conduct Data Protection Impact Assessments ("DPIAs") where required;

4.2.1.6. maintain Records of Processing Activities ("ROPAs");

4.2.1.7. appoint a DPO if required;

4.2.1.8. manage processors through compliant contracts and oversight;



4.2.1.9. conduct legitimate interests assessments where applicable; and

4.2.1.10. embed privacy by design and by default.

4.2.2. Processors must follow documented instructions, ensure security, assist controllers with rights requests and DPIAs, maintain records, notify breaches to controllers without undue delay, and control sub-processing.

4.2.3. The DPO advises the controller's management, monitors compliance, is accessible to data subjects and the ICO, and must be resourced and independent.

Requirements for Data Processing

The core data protection principles shape every stage of the data lifecycle and should be reflected in policies, system design, and day-to-day decision-making.

5.1. Grounds for collection and processing

5.1.1. Processing must be based on one of the lawful bases set out in Art 6 UK GDPR:

5.1.1.1. consent;

5.1.1.2. performance of a contract with the data subject;

5.1.1.3. compliance with a legal obligation;

5.1.1.4. protection of the data subject's vital interests;

5.1.1.5. performance of a public task; or

5.1.1.6. legitimate interests (subject to balancing and transparency).

5.1.2. Special category and criminal offence data require additional conditions (e.g., explicit consent or substantial public interest grounds).

5.1.3. Consent: Under Art 7 UK GDPR, consent must be freely given, specific, informed and unambiguous, and explicit where required (for special category data). Controllers must be able to demonstrate consent and provide mechanisms to withdraw it as easily as it was given. Withdrawal does not affect the lawfulness of processing carried out before withdrawal, but controllers must cease processing that relies on consent and update systems and downstream processors accordingly.

5.2. Transparency obligations

5.2.1. The controller must provide the data subject with clear privacy information. Where the information is collected directly from the data subject, this must be provided at the time of collection (Art 13 UK GDPR). Where the personal data is collected indirectly, then the obligation is to provide the information within one month or when contacting the data subject, whichever is earlier (Art 14 UK GDPR).

5.2.2. The privacy notice should cover processing purposes, lawful bases, categories of data, recipients, international transfers, retention, rights, and contact details/DPO information where applicable. Where consent is relied upon, notices should explain the consequences of refusal/withdrawal and avoid bundled or conditional consents.

5.3. Data storage and retention timelines

The storage limitation principle requires organisations to retain personal data only as long as is necessary for stated purposes, reflected in documented retention schedules aligned to legal, regulatory, tax and sectoral obligations. End-of-life data must be securely deleted or anonymised. Where retention is mandated (e.g., financial or health records), organisations should ensure strict access controls and periodic review.

5.4. Automated decision making

Solely automated decision-making producing legal or similarly significant effects is restricted; exceptions apply where authorised by law, necessary for a contract, or based on explicit consent, with appropriate safeguards including meaningful human review.

5.5. Data protection and security practices and procedures (Chapter IV, Section 2, UK GDPR)

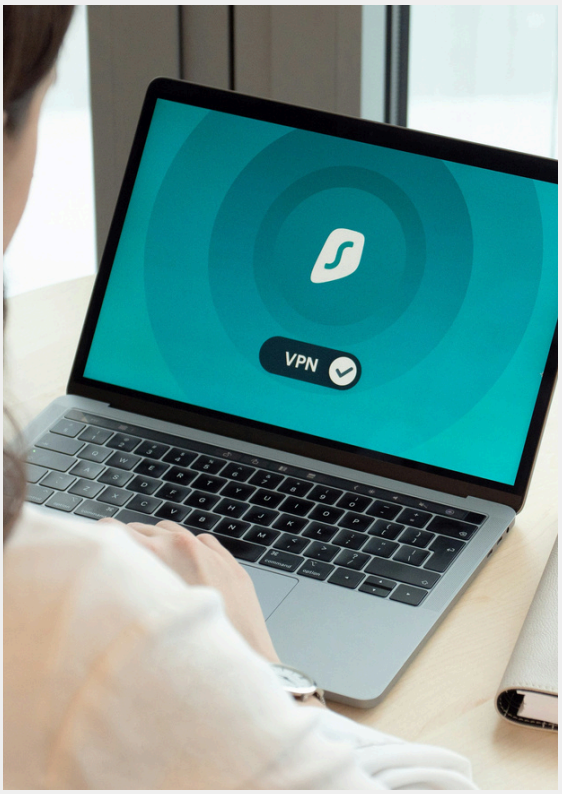
5.5.1. Security measures must be appropriate to risk, considering the likelihood and severity of harm, the nature and sensitivity of data, and processing context. Technical measures typically include encryption, access controls, network security, secure development practices, vulnerability management, and resilience planning. Organisational measures include governance policies, training, supplier due diligence, incident response planning, and periodic assurance. DPIAs are required for high-risk processing (e.g., large-scale sensitive data, systematic monitoring, profiling with significant effects).

5.52. In the event of a personal data breach where there is a risk to individuals' rights and freedoms, controllers must notify the ICO without undue delay and in any event within 72 hours of becoming aware of the breach. In addition, controllers must notify affected individuals without undue delay if the risk to the rights and freedoms of those individuals is high. Breach notifications to the ICO should, where possible, set out the nature of the breach (including categories and approximate number of data subjects and records), likely consequences, measures taken or proposed to address the breach, and a contact point for further information. All breaches—whether notifiable or not—must be logged by the data controller.

5.6. Disclosure, sharing and transfer of data

5.6.1. Data sharing requires a lawful basis, transparency to data subjects, minimisation, and security. Data controllers should document sharing arrangements and determine roles (joint controllers vs separate controllers).

5.6.2. Processor engagements between controllers and processors must be governed by UK GDPR-compliant contracts with mandatory clauses covering subject matter, duration, nature and purpose of processing, confidentiality, security, sub-processing approvals, assistance with rights and DPIAs, audits, and deletion/return at the end of services.



https://www.fladgate.com/

5.7. Cross-border transfer of data

5.7.1. Under Chapter V UK GDPR, transfers of personal data to third countries from the UK require either adequacy regulations (recognising jurisdictions that provide essentially equivalent protection to UK GDPR) or appropriate safeguards, typically the IDTA or the UK Addendum to EU SCCs, together with transfer risk assessments and supplementary measures where necessary. Organisations should assess the legal and practical risk environment in the destination country and document the assessment, implementing technical and organisational measures (such as robust encryption and access controls) where appropriate. Derogations are available only for specific circumstances (e.g., explicit consent after full disclosure of risks, necessary for contract performance, important public interest) but are not appropriate for routine transfers.

5.7.2. Transfers of personal data between the EEA and the UK are the subject of mutual adequacy decisions. The UK generally follows the EU's adequacy decisions.

5.8. Grievance redressal

5.8.1. Controllers are required to maintain accessible internal mechanisms for complaints and rights handling.

5.8.2. Data subjects may escalate their complaints to the ICO if unsatisfied, and have the right to seek judicial remedies and compensation for material and non-material damage caused by infringements.

Rights of Data Subjects

6.1. Rights and remedies

6.1.1. Chapter III of UK GDPR provides data subjects with the following rights:

6.1.1.1. Right to be informed: Data subjects have the right to be informed about how their personal data is being collected and used (see paragraph 5.2)

6.1.1.2 Right of access: Data subjects can request a copy of their personal data held by an organisation. This is also called a "subject access request."

6.1.1.3 Right to rectification: Data subjects can have inaccurate or incomplete personal data corrected.

6.1.1.4 Right to erasure: Also known as the "right to be forgotten", data subjects can request that their personal data be deleted in certain circumstances.

6.1.1.5. Right to restrict processing: Data subjects can request that the processing of their personal data be limited.

6.1.1.6. Right to data portability: Data subjects have the right to obtain their personal data and reuse it for their own purposes across different services.

6.1.1.7. Right to object: Data subjects can object to the processing of their personal data in certain situations, particularly direct marketing.

6.1.1.8. Rights relating to automated decision-making and profiling: Data subjects have the right not to be subject to a decision based solely on automated processing and to obtain information about the reasoning behind such decisions.

6.1.1.9. Right to withdraw consent: If processing is based on consent, data subjects have the right to withdraw their consent at any time.

6.1.2. every data subject has the right to complain to a data controller about the treatment of their personal data, and if the matter is not resolved, under Art 77 UK GDPR, to make a complaint to the ICO.

6.1.3. Under Art 80 UK GDPR, the data subject can mandate a qualifying body or organisation, such as a nonprofit organisation, to complain or take action on their behalf.

6.2. Duties

6.2.1. Data controller

6.2.1.1. As discussed above, the data controller is primarily responsible for compliance with the laws relating to personal data. Controllers must comply with the obligations for processing set out in paragraphs 4.2.1 and 5, as well as taking the steps necessary to ensure that data subject's rights, as set out in paragraph 6.1.1 are respected.

6.2.1.2. It is important that controllers do not see compliance as an afterthought or a matter of producing wordy policies that no-one reads. Art 25 UK GDPR sets out a primary obligation on controllers, to implement systems which are designed to comply with UK GDPR, and to integrate safeguards to meet the requirements of UK GDPR.

6.2.1.3. In addition, Art 5 UK GDPR sets out the "accountability principle": "The controller shall be responsible for, and be able to demonstrate compliance with [the principles set out in 3.1.3]." Therefore, it is not enough to simply comply with UK GDPR; controllers must be able to show that they comply.

6.2.1.4. A further set of obligations is imposed on data controllers under PECR, in relation to electronic marketing. These obligations include:

6.2.1.4.1. a ban on unsolicited electronic marketing, except in limited circumstances, and provided an opt-out mechanism is included; and

6.2.1.4.2. the requirement for consent for the placing of non-essential cookies or similar technology on users' browsers or equipment.

6.2.2. Data processors

Data processors have their own set of responsibilities and are liable in their own right for non-compliance, as well as any contractual obligations or other liability to the controller on whose behalf they are processing personal data. The duties of processors include:

6.2.2.1. Processing Data Only on Instructions: A data processor must process personal data only as instructed by the data controller and must not process data for their own purposes.

6.2.2.2. Security Measures: Ensure that appropriate security measures are in place to protect personal data. This includes both technical and organisational measures to safeguard against unauthorised access, accidental loss, or destruction of data.

6.2.2.3. Confidentiality: Ensure that anyone who can access personal data is under a duty of confidentiality.

6.2.2.4. Sub-processors: Obtain prior written authorisation from the data controller before engaging any sub-processors, and ensure that sub-processors adhere to similar obligations laid out in the processor agreement.

6.2.2.5. Assistance to Data Controllers: Assist data controllers in complying with their UK GDPR obligations. This includes helping with data protection impact assessments and consultations, responding to subject access requests, and ensuring proper breach notification procedures.

6.2.2.6. Data Breach Notification: Inform the data controller without undue delay after becoming aware of a personal data breach.

6.2.2.7. Accountability: Maintain records of processing activities and provide these records to the ICO upon request.

Processing of Children or Minors' Data

7.1. The UK applies a commonly used threshold of 13 years of age for a child to lawfully provide consent to online information society services; below that age, parental consent is generally required in circumstances where consent is the chosen lawful basis for processing.

7.2. The ICO has published a Children's Code, which imposes high privacy defaults, data minimisation, age-appropriate design, and restrictions on profiling or nudging practices that could be detrimental to children's wellbeing.

Regulatory Authorities

8.1. Overview

The ICO is the independent regulator responsible for supervising and enforcing UK GDPR, DPA 2018 and PECR. Other regulators (e.g., communications industry and financial services industry regulators) intersect in sector-specific contexts, but enforcement of data protection laws and PECR resides primarily with the ICO.

8.2. *Role, functions, and powers of the ICO*

8.2.1. The ICO issues guidance, investigates complaints, and exercises corrective and sanctioning powers.

8.2.2. It also operates engagement initiatives (such as regulatory sandboxes and consultations) and increasingly publishes reprimands and enforcement outcomes to drive transparency and improve industry practice.

8.2.3. The ICO has the following powers:

8.2.3.1. Information Notices: The ICO can require organisations to provide information within a specified timeframe.

8.2.3.2. Assessment Notices: The ICO can assess organisations' compliance with data protection principles.

8.2.2.3. Enforcement Notices: The ICO can mandate organisations to take specific actions to comply with the law.

8.2.3.4. Penalties: The ICO can impose administrative fines (see paragraph 9 below).

8.2.3.5. Prohibition Notices: The ICO can prohibit processing activities if they are not compliant with GDPR.

8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

8.3.1. The civil courts have two main functions:

8.3.1.1. To provide a remedy for data subjects, who can bring civil suit against controllers, claiming damages for losses incurred under the UK GDPR or PECR (Reg 30).

8.3.1.2. To enforce any orders of the ICO through court orders and, ultimately, contempt of court.

8.3.2. The criminal courts have a very limited function in relation to the bulk of data protection law in the UK, with the exception of Section 170 of the DPA 2018, which makes it a criminal offence to deliberately disclose or retain personal data without the consent of the controller.

Consequences of non-compliance

The consequences of any infringement of data protection laws can, potentially, be twofold: administrative investigation and sanctions under Art 83 UK GDPR, and/or a civil claim for damages.

9.1. Consequences and penalties for less serious infringements

Lower administrative fines are capped at the higher of £8.7 million or 2% of worldwide annual turnover. These fines may be applied for less serious infringements such as failing to keep adequate records or failing to conduct a DPIA.

9.2. Consequences and penalties for serious non-compliance

The higher administrative fines of £17.5 million or 4% of worldwide annual turnover apply to serious infringements, such as the failure to comply with the basic principles of UK GDPR. The same limits (as of 2025) apply to breaches of PECR.

9.3. ICO approach to penalties

In setting penalties, the ICO considers factors such as the nature, gravity and duration of the infringement, whether it was intentional or negligent, categories of personal data affected, the degree of cooperation, and prior infringements. The ICO can also order suspension or restriction of processing, impose corrective actions, and require notification to affected individuals.

Conclusion

We do not expect considerable divergence between UK GDPR and EU GDPR in the short to medium term and, in general, businesses can often combine compliance programmes for UK and EU entities. Increased consumer awareness of privacy issues means that large processors need to be wary of consumer class actions.

Contact Us

+44 20 3036 7000

https://www.fladgate.com/

epowell@fladgate.com

16 Great Queen Street
London, WC2B 5DG England

USA – Illinois

McDonald Hopkins' national data privacy and cybersecurity attorneys have a wealth of experience advising clients in a myriad of industries on the rapidly changing state, federal, international, and industry privacy and breach notification laws. McDonald Hopkins provides support on a daily basis and during investigations by state and federal regulators, as well assistance with:

- Breach coaching and incident notification
- International privacy compliance
- Payment cards and ecommerce
- Privacy litigation and class action
- Proactive measures and breach compliance
- Regulatory investigation and government response
- Vendor relationships

Introduction

Illinois has enacted laws addressing rights and obligations related to data privacy. Companies and organizations that handle, collect, disseminate, or otherwise deal in nonpublic information have a number of requirements to bolster the data privacy rights and protections of residents. This paper will address the Illinois Personal Information Protection Act (815 ILCS 530/) as well as the proposed Illinois Data Protection and Privacy Act (HB3385).

Governing Data Protection Legislation

Overview of principal legislation – Personal Information Protection Act

The principal data protection legislation in Illinois is the Personal Information Protection Act (815 ILCS 530/) ("PIPA"). PIPA was signed into law in 2005 and took effect in January 2006. The law was later updated to consider changes in technology and data collection methodology.

PIPA applies only to computerized data. Under PIPA, any data collector that maintains or stores, but does not own or license, computerized data that includes personal information as described further below, shall notify the owner or licensee of such information in the event of a breach of a security of the

Contact Us

+1 (312) 280-0111
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
300 N. LaSalle Street, Suite 1400
Chicago, Illinois 60654 USA

data, if the personal information was or reasonably believed to have been acquired by an unauthorized person. This applies regardless of whether the data collector conducts business in Illinois. If notice is issued to more than 500 Illinois residents as a result of a single breach, the data collector must also notify the Attorney General of the breach. PIPA also requires data collectors to maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure.

Additional or ancillary regulation, directives or norms

Illinois Biometric Privacy Act

The Illinois Biometric Privacy Act 2008 ("BIPA") (740 ILCS 14/1 to 740 ILCS 14/99) is significant as it was the first state legislation to address the collection and sharing of biometric information. The Act was passed in 2008, and other states began introducing legislation aimed at addressing biometric data thereafter. An overarching theme of BIPA is that an entity must maintain a reasonable standard of care in managing biometric information.

BIPA provides a set of rules for businesses to follow when collecting biometric data of state residents:

- Prior consent is required before the collection or disclosure of biometric data, such as fingerprints, voiceprints, or scans of hand or face geometry;
- Biometric data must be destroyed in a timely manner; and
- Biometric data must be securely stored.

Student Online Personal Protection Act

The Student Online Personal Protection Act ("SOPPA") (105 ILCS 85/1 to 105 ILCS 85/99) is the student data privacy law that regulates students' covered information by schools, education technology vendors, and the Illinois State Board of Education. It was signed into law in 2019 and outlines specific rights and responsibilities as it relates to covered information.

SOPPA requires that a school must provide notice to the parents of students within 30 days after determining that a breach of covered information occurred. It further requires that schools must implement and maintain reasonable security procedures to protect covered information from unauthorized access, destruction, use, modification, or disclosure. Additionally, SOPPA outlines requirements as to the deletion of covered information.

Upcoming or proposed legislation

After failing in the Illinois House of Representatives in January 2025, The Illinois Data Protection and Privacy Act (HB3385), which was first introduced by Rep. Abdelnasser

Rashid in the 2023 House session, was reintroduced in the 2025-2026 session as HB3041 under the same name. If passed, the bill would implement data minimization practices. Additionally, the bill outlines data subjects' rights, including the right to access, rectification, deletion, data portability, and object to data processing. The bill also includes protections for minors, including a prohibition against engaging in targeted advertising if the covered entity is aware that the individual is a minor, or transferring the data of a minor to a third party without express consent from a parent or guardian. The bill further addresses the establishment of more practical data security practices, such as employee trainings.

If passed, the bill would provide significant protections to Illinois residents.

Legislative Scope of the Illinois Personal Information Protection Act (815 ILCS 530/)

The Illinois general data breach notification statute, PIPA, applies to any data collector that owns or licenses computerized personal information concerning an Illinois resident ("covered entity"). A data collector is any entity that handles, collects, disseminates, or otherwise deals with nonpublic personal information for any purpose, including but not limited to corporations, government agencies, universities, financial institutions, and retail operators.

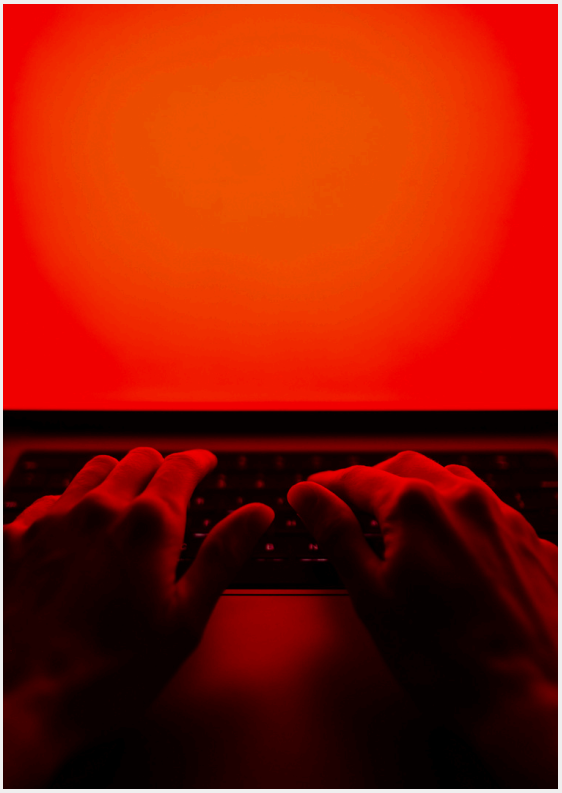
Definition of personal information

Under PIPA, "personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements when not encrypted or redacted:

- Social Security number.
- Driver's license number or State identification card number.
- Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Medical information.
- Health insurance information.
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Personal information also includes a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Of note, personal information does not include publicly available information that is lawfully made available to the general public from government records.



Definition of different categories of personal data

PIPA further defines "health insurance information" to include: an individual's health insurance policy number, subscriber identification number, unique identifier used to identify an individual, medical information in a health insurance application, and claims history.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or treatment or diagnosis by a healthcare professional.

Statutory exemptions

Entities subject to the privacy and security standards outlined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Health Information Technology for Economic and Clinical Health Act ("HITECH") will be in compliance with PIPA's breach notification requirements if they provide a copy of any breach notice sent to Health and Human Services to the Illinois Attorney General within five days.

Territorial and extra-territorial application

PIPA, applies to any data collector that owns or licenses computerized personal information concerning an Illinois resident, regardless of the location of the data collector.

Legislative Framework

Key Stakeholders

Data Collector

"Data Collector" refers to, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any reason, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

A data collector that owns or licenses personal information concerning an Illinois resident is responsible for securely maintaining that information, and notify the resident in the event of a breach of the security of the system data following discovery of the breach. The notification must be made expediently and without unreasonable delay.

Notice to individuals may be provided in one of the following ways:

- Written notice;
- Electronic notice, if it is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
- Substitute notice, if the data collector can demonstrate that the cost of providing notice would exceed $250,000 or if the notice population exceeds 500,000. Substitute notice can also be provided in the event the data collector does not have sufficient contact information. Substitute notice can include:
    - o Email notice;
    - o Conspicuous notice posted on the data collector's web page; or
    - o Notification to major state wide media, or local media if the breach impacts residents in one geographic area.

Notification to more than 500 Illinois residents as a result of a single breach requires the covered entity provide notice to the Attorney General. Such notification must include a description of the breach, the number of Illinois residents impacted, and steps the data collector has taken in relation to the incident. The Attorney General may make this information public.

State Agency

PIPA contemplates the roles and responsibilities of state agencies. Under the statute, any State agency that collects personal information concerning an Illinois resident is required to provide notice in the event of a breach of the security of the system data or written material following discovery of the breach. The notification must be made expediently and without unreasonable delay.

Any State agency that notifies more than 1,000 individuals in connection with a single breach is required to notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p). Further, any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents must provide notice to the Attorney General with the information described above.

Data Brokers

An amendment to PIPA was introduced to the 2025-2026 session, which, in the event it passes, would require "data brokers" in Illinois to register with the Illinois Attorney General's office.

The amendment defines "data brokers" any business "that knowingly collects and sells to third parties the personal information of a customer with whom the business does not have a direct relationship." Notably, data brokers would not include organizations covered by the Fair Credit Reporting Act ("FCRA") or the Gramm-Leach-Bliley Act ("GLBA").

If the amendment to PIPA is passed, data brokers will need to register with the Illinois Attorney General on an annual basis which also includes a registration fee that is to be determined by the Attorney General.

Additionally, data brokers will need to provide the following information:

- The name of the data broker and its primary physical, email, and Internet website addresses;
- Whether the data broker collects the personal information of minors;
- Whether the data broker collects consumers' precise geolocation;
- Whether the data broker collects consumers' reproductive health care data;
- A link to a page on the data broker's website that does not make use of any dark patterns; and
- Whether, and to what extent, the data broker or any of its subsidiaries is regulated by the FCRA or GLBA.

Regulatory Authorities and consequences of non-compliance

The provisions set forth in 815 ILCS §§ 530/1 through 530/25 are enforced by the Illinois Attorney General. Violations of the statute are considered unlawful practices under the Consumer Fraud and Deceptive Business Practices Act and as such are subject to all applicable penalties under the Act. To that end, covered entities that fail to comply with the statutory requirements are subject to both monetary and civil liability penalties. This includes:

- Injunction;
- The inability to conduct business within Illinois;
- Civil penalties up to $50,000;
- Additional penalties of $50,000 per violation;
- Additional penalties of $10,000 per violation for acts committed against a person 65 years or older.

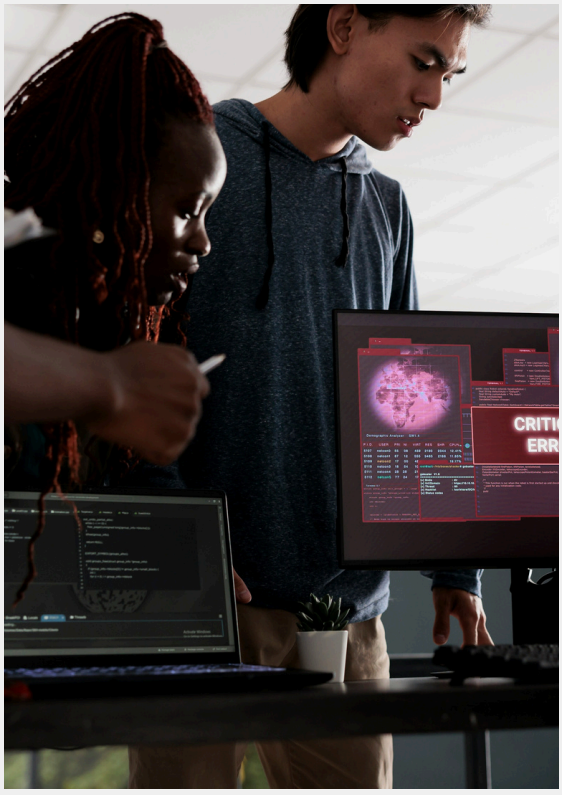
Legislative Scope of the proposed Illinois Data Protection and Privacy Act (HB3385)

The proposed Data Protection and Privacy Act ("DPPA") applies to any entity that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data ("covered entity"). A covered entity does not include a federal, State, tribal, territorial, or local government entity, or an entity acting as a service provider to the aforementioned government entity. The definition also does not include nonprofits, national resource centers, or clearinghouses providing assistance to various vulnerable groups as defined further in the bill.

The DPPA provides that a covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate.

Definition of covered data

Under the DPPA, "covered data" refers to information, including derived data and unique identifiers that identifies or is linked to, alone in combination with other information, to an individual or a device that identifies or is linked to an individual. Covered data does not include de-identified data, employee data, or publicly available information.



Other key definitions

A "data broker" is a covered entity whose principal source of revenue is derived from processing or transferring covered data that the entity did not collect directly from the associated individuals. This does not include employee data collected by and received from a third party for the sole purpose of providing benefits to the employee.

The bill defines "biometric information" as covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that can be linked to the individual. This can include fingerprints, voice prints, retina scans, or hand mapping.

"Collection" refers to the buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

"Control" means an entity that has ownership of another entity, control over a voting majority, or the power to exercise controlling influence over the management of an entity.

A "covered minor" refers to an individual under the age of 17.

To "process" covered data refers to conducting or directing any operation on covered data, including analyzing, organizing, retaining, storing, using, or otherwise handling said data.

"Sensitive covered data" refers to the following:

- A government-issued identifier, such as a Social Security number, passport number, or driver's license number;
- Any information that describes or reveals the health condition or diagnosis of an individual;
- Financial account number or credit or debit card number;
- Biometric information;
- Genetic information;
- Precise geolocation information;
- Private communications such as text messages;
- Account or device log-in credentials;
- Information identifying sexual behaviour;
- Calendar information, address book information, audio recordings, or videos maintained for private use, regardless of what information is contained therein;
- Photos or videos showing nudity or partial nudity of an individual;
- Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service;
- Information about an individual when the covered entity or service provider knows the individual is a covered minor;
- Race, color, ethnicity, religion, or union membership;
- Information identifying an individual's online activity over time and across websites;
- Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data described above.

Extra-territorial application

If passed, the DPPA would apply to covered entities that collect, process, or transfer covered data of Illinois residents, regardless of the location of the entity.

Legislative Framework

Requirements for Data Collection, Processing, or Transfer

Should the DPPA pass, it would only allow for the collection, processing, or transfer of covered data to the extent it is reasonably necessary and proportionate to provide a specific product or service requested by the individual. The bill describes specific scenarios in which data collection, processing, or transfer would be legitimate.

The DPPA also prohibits a covered entity from transferring covered data without obtaining an individual's affirmative express consent. Moreover, an individual must have the means to withdraw any affirmative express consent previously provided with respect to the processing or transfer of covered data. Notwithstanding this, a covered entity that directly engages in collection, processing, or transfer activities enumerated in the bill need not allow opt-out mechanisms.

Under the bill, a covered entity may not collect, process, or transfer data in a discriminatory manner.

Data storage and retention timelines

Covered data must be disposed when it is no longer necessary for the purpose for which it was collected, processed, or transferred, unless an individual has provided affirmative express consent to retention. Such disposal includes permanently destroying or otherwise modifying the data to make it permanently indecipherable.

Data protection and security practices and procedures

The DPPA would require a covered entity to establish, implement, and maintain reasonable data security practices to protect the covered data against unauthorized access or acquisition. If passed, practices should include:

- Identifying and assessing material risks and vulnerabilities in security systems;
- Taking preventative corrective actions to mitigate foreseeable risks;
- Disposing of covered data when it is no longer necessary for the purpose for which it was collected, processed, or transferred, unless affirmative express consent was obtained for additional retention;
- Providing employee training to safeguard covered data;
- Designating an officer to maintain and implement practices;
- Implementing procedures to detect, respond to, and recover from security incidents.

Minors' Data

- A covered entity would not be permitted to engage in targeted advertising to known minors. Moreover, under the bill, a covered entity may not transfer covered data of a covered minor to a third party without affirmative express consent of the minor's guardian, with some exceptions.

https://www.mcdonaldhopkins.com/

Regulatory Authorities

If passed, the DPPA would enable the Attorney General to adopt rules for purposes of carrying out the Act. This would include adjusting definitions, updating or adding categories to definitions, establishing rules and procedures to facilitate an individual's ability to delete or correct covered data, and establishing additional exceptions to protect the rights of individuals.

Additionally, any person subject to a violation of the DPPA could bring a civil action against the violating entity. If the plaintiff prevails, the court may award the plaintiff compensatory, liquidated or punitive damages. In addition, a court could award injunctive relief, declaratory relief, and/or attorney's fees.

Consequences of non-compliance

The Attorney General, State's Attorney, or municipality's attorney may bring a civil action against any covered entity that violates the DPPA. Penalties include:

- Enjoining violating acts;
- Enforcing compliance with the DPPA;
- Obtaining damages, civil penalties, restitution, or other compensation on behalf of residents of Illinois;
- Obtaining reasonable attorneys' fees or other litigation costs.

Conclusion

The Illinois legislative landscape includes robust requirements for data collectors in the event of a data breach. The Illinois Data Protection and Privacy Act includes specific parameters surrounding the protection and breach of resident data. The proposed Data Protection and Privacy Act would add to the privacy landscape in Illinois by providing individuals with increased rights as it relates to their personal data, as well as imposing increased responsibilities on entities that collect, process, and transfer such data.

Contact Us

+1 (312) 280-0111
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
300 N. LaSalle Street, Suite 1400
Chicago, Illinois 60654 USA

USA – Ohio

McDonald Hopkins' national data privacy and cybersecurity attorneys have a wealth of experience advising clients in a myriad of industries on the rapidly changing state, federal, international, and industry privacy and breach notification laws. McDonald Hopkins provides support on a daily basis and during investigations by state and federal regulators, as well assistance with:

- *Breach coaching and incident notification*
- *International privacy compliance*
- *Payment cards and ecommerce*
- *Privacy litigation and class action*
- *Proactive measures and breach compliance*
- *Regulatory investigation and government response*
- *Vendor relationships*

Introduction

In recent years, Ohio has made unique and nationally-mirrored efforts toward advancing a goal of protecting the personal data of its residents. In addition to joining other U.S. states in 2005 by requiring companies to notify consumers of breaches of their personal data,[1] Ohio was the first state in the nation in 2018 to enact legislation – the Ohio Data Protection Act ("DPA") - providing businesses a specific legal incentive to maintain cybersecurity programs for the protection of personal data. A limited number of other jurisdictions, such as Utah, have since taken similar incentive-based approaches to rewarding businesses that take specified action toward enhancing their cybersecurity postures and the protection of personal data.

Additionally, in 2021 Ohio joined the ranks of an expanding set of states across the U.S. that have introduced comprehensive consumer data privacy legislation that, if enacted, would fundamentally change the existing privacy landscape by providing Ohioans with newfound rights pertaining to their personal data. If enacted, OPPA would also impose new requirements on covered businesses to comply with specific privacy and cybersecurity-related requirements such as the posting of a privacy policy and maintenance of physical, technical, and administrative safeguards to protect the security of the personal data.

[1] See Ohio Rev. Code 1349.19

Contact Us

+1 (216) 348-5400
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
600 Superior Avenue E., Suite 2100
Cleveland, Ohio 44114-2653 USA

This article explores the core components of both OPPA and the Ohio DPA, assesses the new requirements for Ohio businesses under this emerging framework, and forecasts the new rights Ohioans may soon enjoy pertaining to the protection of their personal information.

Governing Data Protection Legislation

2.1.Ohio Data Protection Act (DPA) – Existing

In 2018 Ohio took the trailblazing step of enacting the Ohio Data Protection Act (DPA), which provides companies that implement specified cybersecurity programs a legal "safe harbor" in actions against them pertaining to data breaches.

Specifically, the Ohio DPA was the first such law in the nation to offer covered entities who implement specified cybersecurity programs an affirmative defense to specific causes of action sounding in tort.[1] Applicable causes of action must be brought under Ohio law or in Ohio court. Additionally, for the affirmative defense to apply, the cause of action must allege "that failure to implement reasonable information security controls resulted in a data breach concerning personal or restricted information."[2]

Given the ever-increasing cadence of data privacy-related litigation stemming from consumer-plaintiffs whose personal information is involved in data breaches, the Ohio DPA incentivizes Ohio businesses to take steps to protect personal information that they may otherwise not take. Although narrow in scope in that it may apply only after specified allegations are made, the Ohio DPA is unique in that it takes an incentive-based (as opposed to punitive-based) approach to achieve a desired outcome whereby the overall security of consumer data is enhanced through efforts made by companies that process such data to create cybersecurity programs.

2.2.Ohio Personal Privacy Act (OPPA) – Introduced

In addition to its novel enactment of the DPA, Ohio is also following in the footsteps of an expanding set of U.S. states – such as California, Connecticut, Colorado, Utah and others - that have enacted comprehensive consumer data privacy legislation. Specifically, in 2021 Ohio introduced House Bill 376, known as the Ohio Personal Privacy Act ("OPPA"), to the Ohio House of Representatives. If ultimately enacted, OPPA would provide consumers with enumerated and hallmark rights pertaining to the use and maintenance of their personal data that are mirrored in the comprehensive data privacy legislation elsewhere in the country. In addition to affording consumers with specific rights pertaining to the processing of their personal data, OPPA would also require businesses

[1] Ohio Rev. Code, 1354.02(D)
[2] Id.

to maintain safeguards and offer consumers a specified level of transparency with respect to their procedures pertaining to the collection and use of personal data through the conspicuous posting of a privacy policy.

Scope of Application

The Ohio DPA and proposed OPPA both specify the nature of the information that is being protected by the respective legal framework. Only specific information, such as "personal information" as defined under Ohio's DPA or "personal data" as defined under OPPA, rise to the level of triggering certain rights and obligations as applicable.

Additionally, if enacted, OPPA would mirror existing and proposed comprehensive consumer data privacy legislation in limiting its application to certain businesses based on factors such as (1) the connection that the business has to Ohio through physical presence and/or targeting of Ohio consumers, (2) the annual gross revenue of the business, (3) the volume of personal data processed by the business, and (4) amount of revenue the business derives from the sale of personal data.

3.1. Definition of Personal Information and Restricted Information (Ohio DPA)

The incentive-based Ohio DPA incorporates the definition of "personal information" from Ohio's previously-enacted data breach notification statue (Ohio Rev. Code, 1349.19), which defines "personal information" as:

[A]n individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- Social security number;
- Driver's license number or state identification card number; or
- Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.[1]

Under the Ohio DPA, "Personal information" does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records and certain widely-distributed media."[2]

The Ohio DPA also defines "restricted information" as "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to

[1] Ohio Rev. Code, 1347.12(A)(7)(a)
[2] Id.

an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property."[1]

The concepts of both "personal information" and "restricted information' are integral to the foundation of the DPA in that, for a business to enjoy an affirmative defense under the DPA, the legal cause of action brought against the business seeking to employ the affirmative defense must allege a failure to implement reasonable information security controls resulted in a data breach concerning personal or restricted information.[2] Moreover, personal information is foundational to the affirmative defense in that the cybersecurity

[1] Ohio Rev. Code, 1354.01(E)

[2] Ohio Rev. Code, 1354.02(D)

https://www.mcdonaldhopkins.com/

program that is maintained must contains administrative, technical, and physical safeguards for the protection of personal information.[1]

3.2. Definition of Personal Data (OPPA)

If enacted in its current version, OPPA would mirror existing and proposed comprehensive consumer data privacy legislation elsewhere throughout the U.S. in defining "personal data" broadly as "any information that is linked or reasonably linkable to an identified or identifiable consumer and that is processed by a business for a commercial purpose."[2] Personal data would not include "data processed from publicly available sources" or "Pseudonymized, deidentified, or aggregate data."[3]

Statutory Exemptions

If enacted in its current version, OPPA would exempt certain personal data regulated by the Children's Online Privacy Protection Act (COPPA), and protected health information under the Health Insurance Portability and Accountability Act (HIPAA).[4] Additionally, OPPA would not apply to Ohio state agencies, financial institutions governed by the Gramm-Leach-Bliley Act (GLBA), and institutions of higher education. Business to business transactions would also be exempt under OPPA. [5]

[1] Ohio Rev. Code, 1354.02(A)(1)
[2] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly
[3] Id.
[4] Id.
[5] Id.

3.3. Covered Entities – Ohio's DPA

Under the DPA, Ohio extends the benefit of an affirmative defense to "covered entities," which are defined broadly as "a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state (Ohio)."[5]

3.4. Covered Entities - OPPA

If enacted in its current version, OPPA would apply much more narrowly than the DPA only to businesses that either conduct business in Ohio or "produce products or services targeted to consumers in" Ohio)," and that satisfy one or more of the following:

·The business's annual gross revenues generated in Ohio exceed twenty-five million dollars;
·During a calendar year, the business controls or processes personal data of one hundred thousand or more consumers; or
·During a calendar year, the business derives over fifty per cent of its gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand or more consumers.[6]

[5] Ohio Rev. Code, 1354.01(B)
[6] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly

Key Stakeholders

OPPA specifies key stakeholders whose rights and/or obligations are impacted by the respective legislation. OPPA mirrors comprehensive data privacy legislation at the national level in setting forth specific definitions of "business," "processors," and "consumers." The category that a person or entities falls into would ordinarily depend on their relationship and connection to personal data.

Business

Under OPPA "Business" would be mean "any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and regardless of whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, that, alone or jointly with others, determines the purpose and means of processing personal data."[1] Businesses would not include Ohio public entities, political subdivisions or processors to the extent that the processor is acting in the role of a processor.[2]

Processors

Under OPPA, "Processors" would mean a natural or legal person who processes personal data on behalf of a business subject to OPPA.[3] With respect to determining whether a person acts as a "business" or a "processor," OPPA would set forth that this it a fact-based determination dependent on the context in which the personal data is processed.[3]

Consumers

Under OPPA, consumers would mean a "natural personal who is a resident" of Ohio "acting only in an individual or household context." Consumers would not include people acting in a "business capacity" or employment context, such as contractors, job applicants, directors, officers or owners.[5]

[1] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly
[2] Id.
[3] Id.
[4] Id
[5] Id.

New Data Processing and Notice Requirements, Emerging Consumer Rights, and Cybersecurity Programs

If enacted, OPPA would require businesses to adopt a transparent and consumer-focused method of processing personal data. Specifically, under OPPA, businesses would be required to communicate certain core aspects of the way that the business interacts with personal data through conspicuous posting of

a privacy policy. Moreover, if Ohio enacts OPPA, it will join an expanding group of other U.S. states in providing residents with specific rights pertaining to their personal data, such as the rights to request a copy, correction, or deletion of their personal data.

Meanwhile, through Ohio's DPA, Ohio has already joined other U.S. jurisdictions in setting forth parameters for cybersecurity programs. That said, Ohio has taken the unique approach through its DPA of framing the cybersecurity program as an incentive-based eligibility criteria for an affirmative defense as opposed to a requirement enforced through punitive measures.

5.1. OPPA Privacy Policy Requirement

Under OPPA, businesses would be required to provide consumers notice about the personal data that it processes about the consumer. Notice would be in the form of a conspicuously posted privacy policy that would identify:

- the categories of personal data processed by the business;
- the purposes of processing for each category of personal data;
- the categories of sources from which the personal data is collected;
- the categories of processors with whom the business discloses personal data;
- the data retention practices and the purposes for retention;
- ·how individuals can exercise their rights under OPPA;
- how the business will notify consumers of material changes to its privacy policies;
- the categories of any third parties to whom the business sells personal data (if any); and
- · the identities of any affiliates to which personal data may be transferred[1]

5.2. New Consumer Rights Under OPPA

If enacted, OPPA would provide consumers specific rights with respect to the processing and

[1] Id.

maintenance of their personal data. Businesses would be prohibited under OPPA from discriminating against consumers who choose to exercise these rights, such as charging such individuals different prices or rates for goods or services. [1] Processors would be required to assist businesses in responding to consumer requests.[2]

Consumer Right to Request Copy of Personal Data

If enacted, OPPA would mirror existing U.S. comprehensive data privacy legislation in providing consumers the right to request a copy of their personal data that the consumer previously provided to a business. Under the proposed framework, businesses would not be obligated to provide access to a consumer's personal data more than once in a twelve-month period.[3]

Consumer Right to Request Correction of Personal Data

Additionally, if enacted, OPPA would provide consumers the right to request the correction of inaccuracies in the consumer's personal data and businesses would be required to correct any such inaccuracies.[4] A similar right exists in existing comprehensive data privacy legislation in the U.S. and abroad (such as the "right to rectification" under Article 16 of the EU General Data Protection Regulation ("GDPR")).

Consumer Right to Request Deletion of Personal Data

Under OPAA, a consumer's right to request the deletion of their personal data maintained by a business would also be protected. Businesses would be required to comply with deletion requests with limited exceptions, such as the event in which the personal data is necessary for the business to adhere to its written records retention schedule. [5]

Consumer Right to Prevent Sale of their Personal Data

If enacted, OPPA would also provide consumers the right to request a business not to sell the consumer's personal data or process the consumer's personal data for the purpose of targeted advertising.[6] Moreover, businesses that sell personal data or that use processed personal data for the purposes of targeted advertising would be required to provide notice of these facts in a manner to enable consumers to "opt out" of the sale of their personal data and/or the use of their personal data for targeted advertising.[7]

5.3. Cybersecurity Programs Under the Ohio DPA

Under the Ohio DPA, covered entities that are seeking an affirmative defense are required to create, maintain, and comply with a written

[1] Id.
[2] Id.
[3] Id.
[4] Id.
[5] Id.
[6] Id.
[7] Id.

cybersecurity program that (1) contains administrative, technical and physical safeguards for the protection of personal information and that (2) reasonably conforms to an industry recognized cybersecurity framework.[1]

Ohio's DPA notes that the cybersecurity program shall be designed to protect the security of personal information, protect against anticipated threats to the security or integrity of the information, and protect against unauthorized access the personal information.[2] The DPA notes that the scale and scope of a cybersecurity program is appropriate if based on factors such as (1) the size and complexity of the covered entity, (2) the sensitivity of the information to be protected, (3) the nature and scope of the activities of the covered entities, and (4) the resources available to the covered entity.[3]

"Industry recognized" cybersecurity frameworks to which a cybersecurity program may conform include:

- National Institute of Standards and Technology's (NIST) framework for improving critical infrastructure cybersecurity;
- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- The Federal Risk and Authorization Management Program's (FedRAMP) Security Assessment Framework;
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense; or
- International Organization for Standardization / International Electrotechnical Commission's 27000 Family – Information Security Management Systems[4]

[1] Ohio Rev. Code, 1354.02(A)(1)-(2)
[2] Ohio Rev. Code, 1354.02(B)(1)-(3)
[3] Ohio Rev. Code, 1354.02(C)(1)-(5)

5.4. New Data Protection Requirements Under OPPA

Under OPPA, processors would be required to maintain "reasonable" administrative, technical, and physical safeguards to protect the security and confidential of personal data.[5] OPPA notes that safeguards

[4] Ohio Rev. Code, 1354.03(A)(1)
[5] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly

shall reflect the nature and scope of the activities of the processor and its role in possessing the personal data.[1] Unlike other privacy legal frameworks such as HIPAA that require covered entities to implement administrative, technical, and physical safeguards, OPPA does not narrowly specify the applicable safeguards, which presumably may entail actions such as monitoring of information systems, employee training on cybersecurity, or requirements with respect to implementation of policies/procedures beyond the core privacy policy.

5.5. Data Processing of Minors' Data

Under OPPA, businesses would be prohibited from selling the personal data collected online of a known child without complying with the requirements or exceptions of the Children's Online Privacy Protection Act of 1998 (COPPA).[2] This requirement mirrors comprehensive data privacy legislation in other jurisdiction, such as Connecticut and other jurisdictions that afford special protections to the personal data of minors.

[1] Id.
[2] Id.

OPPA Enforcement

Unlike similar legislation in other jurisdictions, OPPA does not establish a new privacy regulator. If enacted in its current form, the Ohio Attorney General would maintain exclusive authority to enforce OPPA through investigation of businesses and processors for compliance and civil penalties of up to five thousand dollars for each violation.[3]

If the attorney general has reasonable cause to believe that a business or processor has engaged or is engaging in an act or practice that violates OPPA, the attorney general would be able to bring an action in an Ohio court of common pleas to seek relief in the form of declaratory judgements that the business/processor has engaged in an act or practice that violates OPPA as well as injunctive relief (both preliminary and permanent) to prevent further violations and compel compliance.[4]

[3] Id.
[4] Id.

Conclusion

Ohio is advancing toward a data protection landscape in which it simultaneously promotes and requires the safeguarding of personal data of its residents through collective legislation based in both incentives and requirements. At the aggregate level, Ohio's data protection legislation is focused on rewarding businesses for taking steps to enhancing their cybersecurity posture while also affording consumers newfound control over their personal information and imposing requirements of companies with respect to data processing.

Through enacting an incentive-based DPA, Ohio took the bold and unprecedented step in rewarding businesses that focus on enhancing their cybersecurity postures. That said, an incentive-based program has limitations. Through OPPA, Ohio would round out its data protection legislation by mirroring recent and similar legislation across the U.S. in affording consumers with specific rights pertaining to the handling of their personal data, requiring the declaration of practices pertaining to processing of personal data through the posting of a privacy policy, as well as requiring the maintenance of administrative, technical, and physical safeguards.

Contact Us

+1 (216) 348-5400
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
600 Superior Avenue E., Suite 2100
Cleveland, Ohio 44114-2653 USA