PANORAMIC

DATA PROTECTION & PRIVACY

Luxembourg

LEXOLOGY

Data Protection & Privacy

Contributing Editors
Aaron P Simpson and **Lisa J Sotto**
Hunton Andrews Kurth LLP

Generated on: September 5, 2025

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

Explore on **Lexology**

Contents

Data Protection & Privacy

LAW AND THE REGULATORY AUTHORITY

Legislative framework
Data protection authority
Cooperation with other data protection authorities
Breaches of data protection law
Judicial review of data protection authority orders

SCOPE

Exempt sectors and institutions
Interception of communications and surveillance laws
Other laws
PI formats
Extraterritoriality
Covered uses of PI

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds
Legitimate processing – types of PI

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency
Exemptions from transparency obligations
Data accuracy
Data minimisation
Data retention
Purpose limitation
Automated decision-making

SECURITY

Security obligations
Notification of data breach

INTERNAL CONTROLS

Accountability
Data protection officer
Record-keeping
Risk assessment
Design of PI processing systems

REGISTRATION AND NOTIFICATION

Registration
Other transparency duties

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers
Restrictions on third-party disclosure
Cross-border transfer
Further transfer
Localisation

RIGHTS OF INDIVIDUALS

Access
Other rights
Compensation
Enforcement

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

SPECIFIC DATA PROCESSING

Cookies and similar technology
Electronic communications marketing
Targeted advertising
Sensitive personal information
Profiling
Cloud services

UPDATE AND TRENDS

Key developments of the past year

Contributors

Luxembourg

Simmons & Simmons

Camille Saettel camille.saettel@simmons-simmons.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Luxembourg's data protection framework is built on European Union law and specific national laws. The primary laws currently in force include:

- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR);
- Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection framework (which implements the GDPR);
- Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters (which transposes the Law Enforcement Directive (EU) 2016/680 of 27 April 2016);
- Law of 1 August 2018 on the processing of passenger name record data in the context of the prevention and suppression of terrorism and serious crime (which transposes the EU Passenger Name Record Directive (EU) 2016/681 of 27 April 2016);
- Law of 17 August 2018 on archiving; and
- Amended Law of 30 May 2005 concerning the specific provisions for the protection of the individual in respect of the processing of personal data in the electronic communications sector (which transposes ePrivacy Directive 2002/58/EC of 12 July 2002).

Law stated - 4 May 2025

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The National Commission for Data Protection (CNPD) has been designated as the authority responsible for monitoring and verifying whether data is processed in accordance with:

- the GDPR;
- the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection framework;
- the Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters; and
- legal texts containing specific provisions relating to personal data protection.

The CNPD has the investigative powers provided for in article 58 of the GDPR. Furthermore, pursuant to the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection framework, it has notably the following investigative powers:

- to obtain from controllers and/or processors access to all personal data processed and all information necessary for the performance of its tasks;
- to issue warnings to a controller or a processor that planned data processing operations are likely to infringe provisions adopted pursuant to the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters;
- to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters;
- to impose a temporary or definitive limitation, including a ban, on processing; and
- to advise the controller in accordance with the prior consultation procedure referred to in Article 27 of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters.

Law stated - 4 May 2025

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The CNPD, as a data protection authority, is required to provide other data protection authorities (DPAs) with relevant information and mutual assistance in order to implement and apply the GDPR in a consistent manner (articles 57.1(g) and 61 GDPR). It must put in place measures for effective cooperation with other DPAs. Mutual assistance must cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

Where processing affects data subjects in more than one EU member state (cross-border processing), the lead supervisory authority (which could be the CNPD) must cooperate with the other DPAs concerned (article 60 GDPR). The lead supervisory authority and the other supervisory authorities concerned must seek consensus, exchange all relevant information with each other, and follow the consistency mechanism outlined in article 63 GDPR if a disagreement arises.

The CNPD must also conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the other member states DPAs are involved (article 62 GDPR). The competent DPA must invite the other member states DPAs to take part in the joint operations and must respond without delay to a DPA request to participate.

Luxembourg law reflects these obligations (article 42 of the Law of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework).

Law stated - 4 May 2025

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Data breaches can lead to administrative sanctions under the GDPR. The CNPD may impose administrative fines as set out in article 83 of the GDPR, including in relation to data breaches – for example, obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR), obligation to notify personal data breaches to the competent DPA (article 33 GDPR), obligation to inform affected data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms (article 34 GDPR). Administrative fines may vary depending on the infringed GDPR provision, between €10 million or 2 per cent of global annual turnover and €20 million or 4 per cent of global annual turnover (article 83 GDPR). The method used to calculate fines for private companies is based on the European Data Protection Board's Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

Data breaches can also lead to corrective measures, including warnings, reprimands, temporary or definitive limitations (including a ban) on processing, suspension of data flows to a recipient in a third country, and an order to communicate a personal data breach to the data subject (article 58.2(e) GDPR).

The CNPD adopted, by two decisions dated 23 February 2024, a regulation concerning the investigation procedure and an internal regulation. Breaches are first handled through an investigation step. It starts upon the notification of the breach (by the controller), or with a complaint, or *ex officio* at the CNPD's own initiative. The opening of an investigation may be proposed at any time by a member of the CNPD college. The CNPD may notably conduct on-site audits and request information/documents. The investigation is carried out both for the prosecution and the defence. The data controller has the right to be heard. After the investigation, the CNPD issues a formal written decision, which may include a fine, an order to implement specific measures, and publication of the breach or sanction in serious cases. For cross-border breaches, the CNPD cooperates with other DPAs and, if a disagreement arises, the European Data Protection Board can issue a binding decision (articles 63 to 65 of the GDPR).

Law stated - 4 May 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Decisions issued by the CNPD may be appealed before the Luxembourg Administrative Tribunal.

Law stated - 4 May 2025

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Data protection rules apply to all sectors and types of organisation, whether in the private or public sector (a controller may be, within the meaning of the General Data Protection Regulation (GDPR), any natural or legal person, public authority, agency or another body), and whether the processing is operated by automated means or by non-automated means.

However, data protection rules do not apply to the processing of personal data by an individual in the course of a purely personal or household activity (article 2.2(c) GDPR).

The processing of personal data by competent authorities for the purposes of law enforcement and criminal justice, as well as in matters of common foreign and security policy, is not covered by the GDPR but by the Luxembourg Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters. The processing of personal data by EU institutions, bodies, offices and agencies is neither covered by the GDPR nor a national law but by Regulation (EC) No 45/2001.

Law stated - 4 May 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Data protection rules cover the interception of communications, electronic marketing and the monitoring and surveillance of individuals.

Interception and surveillance:

In accordance with the ePrivacy Directive, the Luxembourg Law of 30 May 2005 concerning specific provisions for the protection of the individual in respect of the processing of personal data in the electronic communications sector (ePrivacy Law) generally prohibits listening, intercepting, storing, or otherwise subjecting communications and related traffic data to interception or surveillance without the consent of the user concerned.

This prohibition has certain exceptions. For example, it does not apply to judicial authorities acting within the scope of the powers assigned to them by law and those competent under the Code of Criminal Procedure to safeguard state security, defence, and public safety and for the prevention, investigation, detection and prosecution of criminal offences (article 4, ePrivacy Law).

Electronic marketing

In accordance with the ePrivacy Directive, the ePrivacy Law requires the prior consent of the user for the use of automated calling and communication systems without human intervention (automatic calling machines), fax machines or electronic mail for direct prospecting purposes (article 11(1), ePrivacy Law). Some specific exceptions may apply.

Law stated - 4 May 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

In addition to the general data protection legislative framework indicated above, Luxembourg has several sector-specific laws and regulations that provide data protection rules in related areas. These include but are not limited to:

- AML/CFT area: The amended Law of 12 November 2004 on the fight against money laundering and terrorist financing contains provisions relating to personal data that is processed by professionals of the basis on this law (article 3(6a), AML/CTF Law);
- Employment area: The Luxembourg Labour Code contains a specific Title relating to the processing of personal data for the purpose of monitoring employees in the context of employment relationships. The Luxembourg Labour Code requires notably that the following be informed in advance by the employer: for individuals subject to the legislation on private law contracts: the joint committee or, failing that, the staff delegation or, failing that, the Labour and Mines Inspectorate (articles L. 261-1 and the following, Luxembourg Labour Code);
- Financial sector area: the Law of 5 April 1993 on the financial sector, as well as Circulars CSSF (notably the Circular CSSF 17/655), contain several personal data protection provisions applicable to professionals of the financial sector, including on personal data processed after a whistleblowing reporting through internal channels;
- Insurance area: The amended Law of 7 December 2015 on the insurance sector contains several provisions relating to personal data protection, including one recently added, allowing insurance companies to lawfully process health data when such processing is necessary for the execution of pre-contractual measures in insurance or reinsurance matters or for the execution of an insurance or reinsurance contract (processing legal basis – article 6.1b, GDPR), in view of the important reasons of public interest inherent in insurance and reinsurance contracts (legal basis for the processing of health personal data – article 9.2g), GDPR);
- Whistleblowing law: In accordance with the Directive (EU) 2019/1937, the Law of 16 May 2023 on the protection of persons who report violations of EU law contains one specific provision relating to the processing of personal data carried out under this law, including the exchange or transmission of personal data by competent authorities.

Law stated - 4 May 2025

PI formats

What categories and types of PI are covered by the law?

The GDPR defines personal data as any information relating to an identified or identifiable natural person. This definition is unchanged under national Luxembourg law. Almost all categories and types of PI are covered by the law. In accordance with the GDPR, the following PI types are notably excluded:

- data relating to legal persons (article 4(1) GDPR);
- personal data of deceased persons (Recital (27) GDPR);
- purely personal or household data (article 2.2(c) GDPR);
- anonymous data (Recital (26) GDPR);
- non-personal information, in statistical and research data (Recital (26) GDPR).

Law stated - 4 May 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

In accordance with the GDPR, the law may have an extraterritorial effect. It applies to the processing of personal data of data subjects who are in the EU, even if the controller or processor is not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The law may also have an extraterritorial effect even where the processing activities are not related to those two situations – for example, a controller or processor may be deemed to have an 'establishment' in Luxembourg (and, therefore, be subject to its law) if it has there a real and effective activity — even a minimal one — exercised through stable arrangements (eg, Recital (22) GDPR).

Law stated - 4 May 2025

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Almost all processing or use of personal data is covered, with the exception of processing activities carried out on types of data not covered by the law (see above). In accordance with

the GDPR, the law makes a distinction between those who control personal data (controllers) and those who provide processing services to owners (processors).

The 'controller' is any entity that, alone or jointly with others, determines the purposes and means of the processing of personal data (it decides on the 'why' and 'how'). The 'processor' is any entity which processes personal data on behalf of the controller based on a contract under EU or Luxembourg law.

The duties of controllers and processors differ. Some examples of this are as follows:

- the controller has a primary responsibility for legal compliance with the data protection rules. The processor must act on documented instructions from the controller;
- the controller must identify and document the processing legal basis. The processor does not need any independent lawful basis for its activity (it relies on the one identified by the controller);
- the controller must respond to the exercise of data subject rights. The processor must assist the controller in fulfilling those rights; and
- the controller must notify the CNPD within 72 hours of becoming aware of a data breach, and the data subjects if necessary. The processor must notify the controller of the data breach without undue delay.

Law stated - 4 May 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

In accordance with the General Data Protection Regulation (GDPR), legal provisions require the processing of personal information (PI) to be legitimised on specific GDPR legal bases. Article 6(1) GDPR lists these legal bases. At least one of the following must apply:

- Consent: Under the GDPR, consent must be based on a clear affirmative action and be freely given, specific, informed and unambiguous. Consent language hidden in terms and conditions, pre-ticked boxes or consent inferred from silence are not valid. Also, consent is unlikely to be valid where there is a clear imbalance of power between the individual and the data controller seeking the consent, such as in employment matters. Electronic consent is acceptable, but it must be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent.
-

Contract: Processing is necessary for the performance of a contract with an individual. This means it is objectively indispensable for a purpose that is integral to the contractual obligation intended for the individual.

- Legal obligation: Processing is necessary for compliance with the controller's legal obligations.
- Vital interests: Processing is necessary to protect the vital interests of a natural person.
- Public task: Processing is necessary to fulfil a task in the public interest or in the exercise of official authority.
- Legitimate interests: Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests or fundamental rights and freedoms of the data subject are overridden. Public authorities cannot rely on this last legal basis in the performance of their tasks.

Law stated - 4 May 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

In accordance with the GDPR, the processing of special categories of personal data is generally prohibited. These special categories of personal data are:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health data; and
- data concerning a person's sex life or sexual orientation.

The categories may only be processed in specific cases and where special conditions are ensured (eg, implemented technical and organisational measures must be appropriate to the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing).

The specific cases are the following:

- the individual has given explicit consent;
- processing is necessary for employment or social protection law;
- processing is necessary for the vital interests of a natural person;
- processing is carried out by and in the context of a non-profit organisation with a political, philosophical, religious or trade union aim;

- processing is related to personal data made public by the individual;
- processing is necessary for legal claims or when courts act in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for health or social care purposes;
- processing is necessary for public health reasons; and
- processing is necessary for archiving, research, or statistics purposes.

Additionally, the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by law.

Law stated - 4 May 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The privacy notice must contain the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- the recipients or categories of recipients of the personal data, if any;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

When personal data has not been obtained from the data subject, supplementary information must be provided, including the categories of personal data concerned by the processing.

Law stated - 4 May 2025

Exemptions from transparency obligations
When is notice not required?

The information notice is generally required before personal data are obtained. However, certain situations allow for exemptions from the obligation to provide notice about the processing of personal data. These exemptions are set out in articles 13(4) and 14(5), General Data Protection Regulation (GDPR). For example, no notice is required where the data subject already possesses the relevant information. The information notice is also not required:

- if personal data have not been obtained from the data subject; and
- if one of the following situations is applicable:
  - the data subject already has the information (article 14.5(a), GDPR);
  - information provision of such information proves impossible or would involve a disproportionate effort (article 14.5(b), GDPR);
  - where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or member state law, including a statutory obligation of secrecy (article 14.5(d), GDPR).

Law stated - 4 May 2025

Data accuracy
Does the law impose standards in relation to the quality, currency and accuracy of PI?

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay (article 5.1(d), GDPR).

Law stated - 4 May 2025

Data minimisation
Does the law restrict the types or volume of PI that may be collected?

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (article 5.1 (c), GDPR).

Law stated - 4 May 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (article 5.1 (e), GDPR).

Law stated - 4 May 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; however, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes (article 5.1 (b), GDPR). The purposes of the processing should be defined before any processing of personal data.

Law stated - 4 May 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

The GDPR provides a few exceptions, including if the automated processing:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by European Union or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

Law stated - 4 May 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Both data controllers and data processors are subject to security obligations to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. They must implement technical and organisational measures that ensure a level of security appropriate to the risk (article 32), which may include encryption, pseudonymisation, ensuring the confidentiality, integrity and availability of systems, and regular testing of security controls.

Data processors may only process personal data on documented instructions from the controller (article 28). They must also ensure that any sub-processors implement appropriate technical and organisational measures. The data processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. It must take all appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as stipulated in the data processing contract concluded with the controller.

Law stated - 4 May 2025

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

A data breach occurs when breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pursuant to the General Data Protection Regulation (GDPR), the law includes the obligation for the controller to notify the personal data breach to the supervisory authority competent (which may be the National Commission for Data Protection) without undue delay and, where feasible, not later than 72 hours after having become aware of it. This obligation applies if the personal data breach is likely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it must be accompanied by reasons for the delay. Where, and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller must also communicate the personal data breach to the data subjects without undue delay whenever the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the information and measures taken to address it. This does not apply if:

-

the controller implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Law stated - 4 May 2025

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Controllers (and processors) are required by law to implement controls ensuring they are responsible and accountable for personal data and demonstrate compliance. In accordance with the General Data Protection Regulation (GDPR), accountability is a core principle: the controller is responsible for and must be able to demonstrate compliance with all data protection principles. In practice, organisations must put in place appropriate governance measures.

In accordance with the GDPR, controllers are further obliged to implement appropriate technical and organisational measures to ensure and demonstrate that processing is performed in accordance with the GDPR rules (article 24, GDPR). Key examples of such controls include maintaining documentation and records and enforcing security safeguards. Controllers (and processors) are required to keep a record of processing activities, documenting what personal data they hold, purposes, recipients, among others, as evidence of compliance (article 30, GDPR). Appropriate security measures (technical and organisational) must also be implemented to protect personal data, proportionate to the risk, such as encryption, access controls, and regular security testing (article 32, GDPR). Other measures such as data protection impact assessments or appointing a data protection officer may also be necessary in certain cases.

Law stated - 4 May 2025

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The appointment of a data protection officer is mandatory only in specific cases where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing, on a large scale, special categories of data and personal data relating to criminal convictions and offences.

The data protection officer has at least the following legal responsibilities:

- to inform and advise the controller or the processor and the employees who carry out the processing of their obligations pursuant to the GDPR and to other EU or member state data protection provisions;
- to monitor compliance with the GDPR, with other EU or member state data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including for the prior consultation referred to in article 36 of the supervisory authority where a data protection impact assessment indicates that the processing would result in a high risk, and to consult, where appropriate, with regard to any other matter.

The data protection officer must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil its tasks under the GDPR. The controller and the processor must ensure that the data protection officer is involved in all issues which relate to the protection of personal data. The controller and processor must support the data protection officer in performing its tasks by providing resources necessary to carry out its tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. The controller and processor must ensure that the data protection officer does not receive any instructions regarding the exercise of its tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing its tasks. The data protection officer directly reports to the highest management level of the controller or the processor.

Law stated - 4 May 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Each controller and, where applicable, the controller's representative must maintain a record of processing activities under its responsibility (article 30.1, GDPR). This record must contain, in particular, a description of the processed categories of personal data. Each processor and, where applicable, the processor's representative must also maintain a record of all categories of processing activities carried out on behalf of a controller (article 30.2, GDPR). However, this record does not need to contain a description of the processed categories of personal data.

The foregoing obligations to maintain a record do not apply to an enterprise or an organisation 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 or personal data relating to criminal convictions and offences.

Law stated - 4 May 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

A risk assessment (data protection impact assessment) is mandatory only in specific cases where:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
- a systematic monitoring of a publicly accessible area on a large scale.

Law stated - 4 May 2025

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

Pursuant to the GDPR, there are explicit obligations on how personal data processing systems must be designed and configured, known as Data protection by design and by default (article 25, GDPR). The controller must implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the GDPR requirements and protect the rights of data subjects.

Measures must be built into systems at the time of the determination of the means for processing and during the processing itself.

Law stated - 4 May 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Controllers and processors are not required to register with the supervisory authority.

Law stated - 4 May 2025

Other transparency duties

Are there any other public transparency duties?

Other than the information published in Data Protection Notices (articles 13 or 14, General Data Protection Regulation (GDPR), the controller or processor must publish the contact details of the data protection officer and communicate them to the supervisory authority (article 37.7, GDPR).

The controller must also inform data subjects of a personal breach in case it is likely to result in a high risk to the rights and freedoms of natural persons (article 34.1 GDPR). Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must also consult the supervisory authority prior to processing (article 36.1, GDPR).

Law stated - 4 May 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The sharing of personal data with entities providing outsourced processing services is regulated primarily by the General Data Protection Regulation (GDPR) as follows:

- a written contract (article 28, GDPR) must be in place between the data controller and the processor, outlining their respective obligations;
- the controller must perform a due diligence and ensure the processor provides sufficient guarantees to implement appropriate technical and organisational measures;
- the processor needs prior written authorisation from the controller to engage sub-processors, unless a general written authorisation has been granted to it; and
-

if data is transferred outside the EU/EEA, appropriate safeguards must be used (eg, adequacy decision from the European Commission, Standard Contractual Clauses, etc).

Law stated - 4 May 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Sharing personal data with such recipients requires a legal basis, the determination of a purpose, compliance with transparency obligations, data minimisation, and the obligations applicable to international transfers if the data subject is outside the EU/EEA. Special categories of data are also subject to specific restrictions. All these and other questions should be addressed in a document – for example, an arrangement between two or more joint controllers (article 26.1, GDPR).

Law stated - 4 May 2025

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The transfer of personal data outside Luxembourg is restricted in certain cases :

- Personal data can freely flow within the EU/EEA, subject to a contract concluded with the processor or controller or joint controller.;
- Personal data transfers outside the EU/EEA are restricted and can only take place if the conditions laid down in Chapter V 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. One of the conditions provided by this Chapter and permitting a transfer of personal data is if the European Commission has issued an adequacy decision, indicating that the third country provides an adequate level of protection for personal data.

Law stated - 4 May 2025

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The same GDPR rules apply equally to transfers to service providers (processors) and onward transfers (eg, transfers from a processor to its sub-processor or another third party).

The Chapter V GDPR applies to any transfer to a third country, regardless of whether the recipient is a controller, a processor, or a sub-processor.

The data exporter (controller or processor in the EU) must ensure that the recipient outside the EU/EEA provides an adequate level of protection or, if not, ensure there are appropriate safeguards in place.

Specifically regarding processors, the GDPR requires them to process data only on the controller's documented instructions, which must include rules on international transfers.

Onwards transfers by non-EU recipients are allowed if they are covered by the same safeguards described above (eg, standard contractual clauses), and the controller maintains oversight and control over the data flow.

Law stated - 4 May 2025

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Under EU and Luxembourg law, there is no general requirement for personal data or a copy of it to be retained in Luxembourg if it is transferred or accessed from outside the country. However, certain exceptions may apply as follows:

- sector-specific laws may impose local data residency or retention obligations for supervisory or security reasons;
- organisations must ensure that the CNPD and other competent authorities can access the data, if needed, for compliance or oversight; and
- the controller remains responsible for ensuring that the data, even if stored or processed abroad, is subject to appropriate safeguards and remains under effective control in line with the GDPR. At the choice of the controller, the processor must delete or return all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless EU or member state law requires storage of the personal data.

Law stated - 4 May 2025

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

In accordance with the General Data Protection Regulation (GDPR), the data subject has the right:

-

to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, to access to the personal data, and

- to obtain the following information:
  - the purposes of the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  - the right to lodge a complaint with a supervisory authority;
  - where the personal data are not collected from the data subject, any available information as to their source; and
  - the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

The controller must provide information on action taken on a data access right request to the data subject without undue delay and, in any event, within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject requests by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Law stated - 4 May 2025

Other rights
Do individuals have other substantive rights?

In accordance with the GDPR, the data subject has the right to request from the controller the rectification of personal data, or the erasure of personal data, or the restriction of processing concerning the data subject, or to object to processing of personal data, as well as the right to data portability. Where a processing is based on consent, the data subject also has the right to withdraw consent at any time, without affecting the lawfulness of processing based

on consent before its withdrawal, as well as the right to lodge a complaint with a supervisory authority. The data subject has also the right to human intervention in decision-making processes.

Law stated - 4 May 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered. Any controller involved in processing is liable for the damage caused by processing, which infringes the GDPR. A processor is liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor is exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor is held liable for the entire damage in order to ensure effective compensation of the data subject. Where a controller or processor has paid full compensation for the damage suffered, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of the responsibility for the damage.

Court proceedings for exercising the right to receive compensation are brought before the competent courts (which competence may depend on the damage suffered).

Law stated - 4 May 2025

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Substantive rights may be enforced through a complaint lodged with the supervisory authority of the data subject's habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data infringes the GDPR. This supervisory authority may be the CNPD.

This enforcement through a complaint is without prejudice to any other administrative or judicial remedy. Each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them or where the supervisory authority does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged.

However, it is not possible to exercise concurrent proceedings. Thus, a complaint procedure before the National Commission for Data Protection will only be admissible if it is not simultaneously the subject of a procedure before a court or another procedure.

Law stated - 4 May 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The law includes several derogations, exclusions, and limitations beyond those already described.

These include special allowances for freedom of expression and information (media/journalistic data processing), for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, and for specific contexts such as employment and professional secrecy. Each derogation is grounded in a General Data Protection Regulation provision (eg, articles 85-90 or article 23) and reflected in Luxembourg's Law of 1 August 2018.

Law stated - 4 May 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of ‘cookies’ or equivalent technology?

Pursuant to the ePrivacy Directive, it is prohibited for anyone other than the concerned user to listen to, intercept, or store communications and related traffic data or to subject them to any other means of interception or surveillance without the consent of the concerned user. This prohibition does not apply to the storage of information or obtaining access to information already stored in the terminal equipment of a subscriber or user, provided that the subscriber or user has given their consent and has received clear and comprehensive information in this regard, including the purposes of the processing. The methods chosen to provide the information and offer the right to refuse should be as user-friendly as possible. Where technically possible and effective, the consent of the subscriber or user may be expressed by using the appropriate settings of a browser or another application.

The above does not prevent technical storage or access exclusively aimed at carrying out the transmission of a communication over an electronic communications network or is strictly necessary for the provider to supply an information society service explicitly requested by the subscriber or user. Technical storage or access for these purposes are based on legitimate interests and do not require the consent of the concerned user.

Law stated - 4 May 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Pursuant to the ePrivacy Directive, the use of automated calling and communication systems without human intervention (calling machines), fax machines, or email for direct marketing purposes is only possible if it targets the subscriber or user who has given prior consent. However, a provider who, in the context of selling a product or service, has obtained the electronic contact details of their customers for email purposes may use these electronic contact details for direct marketing of similar products or services that they themselves provide, provided that these customers are clearly and expressly given the right to object, free of charge and in a simple manner, to such use of electronic contact details when they are collected and with each message, in case they have not initially refused such use.

Unsolicited commercial communication by email must be identified as such in a clear and unambiguous manner as soon as it is received by the recipient.

It is prohibited to send electronic messages for direct marketing purposes by disguising, concealing, or distorting the identity of the sender on whose behalf the communication is made or without providing a valid address to which the recipient can send a request to stop such communications.

Anyone who contravenes the above is subject to imprisonment for eight days to one year and a fine of €251 to €125,000, or one of these penalties.

Law stated - 4 May 2025

Targeted advertising

Are there any rules on targeted online advertising?

Targeted online advertising is subject to data protection and ePrivacy rules. Under the General Data Protection Regulation (GDPR), using personal data for targeted ads typically requires a valid lawful basis - in practice, this is often consent, especially when it involves tracking individuals across websites (profiling) or using third-party advertising cookies. The GDPR's profiling and transparency provisions apply. Notably, individuals have a right to object at any time to the processing of personal data which is based on public interests or legitimate interests, including profiling.

If targeted advertising involves automated profiling that 'significantly affects' individuals, it may trigger the application of article 22 of the GDPR restrictions: data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

Separately, the ePrivacy Directive requires prior user consent before storing or accessing information on a user's device for advertising (eg, cookies for personalised ads). Luxembourg's National Commission for Data Protection (CNPD) published guidelines on cookies and other tracking devices. It has affirmed that non-essential cookies used for advertising require opt-in consent.

Law stated - 4 May 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

In accordance with the GDPR, the processing of special categories of personal data is generally prohibited. These special categories of personal data are:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health data; and
- data concerning a person's sex life or sexual orientation.

The categories may only be processed in specific cases and where special conditions are ensured (eg, implemented technical and organisational measures must be appropriate to the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing).

The specific cases are the following:

- the individual has given explicit consent;
- processing is necessary for employment or social protection law;
- processing is necessary for the vital interests of a natural person;
- processing is carried out by and in the context of a non-profit organisation with a political, philosophical, religious or trade union aim;
- processing is related to personal data made public by the individual;
- processing is necessary for legal claims or when courts act in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for health or social care purposes;
- processing is necessary for public health reasons; and
- processing is necessary for archiving, research, or statistics purposes.

Additionally, the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by law.

Law stated - 4 May 2025

Profiling

Are there any rules regarding individual profiling?

Profiling is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

The data subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data that is based on public interests or on legitimate interests, including profiling. The controller cannot process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data cannot be processed for such purposes. At the latest, at the time of the first communication with the data subject, the right must be explicitly brought to the attention of the data subject and must be presented clearly and separately from any other information.

The data subject cannot generally be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. Except if such decision is:

- necessary for entering into, or performance of, a contract between the data subject and a data controller;
- authorised by Union or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's explicit consent.

In these cases, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Data subjects must be informed of the existence of automated decision-making, including profiling, and have the right to meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Law stated - 4 May 2025

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

Luxembourg entities must adhere to both general data protection rules and sector-specific guidance when using cloud services. General data protection rules apply – for example, if

a cloud provider processes personal data, the controller must ensure a GDPR-compliant processing agreement, appropriate security, and lawful data transfers.

In regulated sectors, specific rules exist. Financial institutions follow European guidelines on cloud outsourcing (from the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority), which Luxembourg's regulators (such as the CSSF) have implemented. These require thorough risk assessments and contractual safeguards (eg, audit rights, data location controls, subcontractor obligations, exit strategies) for cloud arrangements.

Moreover, the Digital Operational Resilience Act became applicable in 2025, introducing uniform requirements on ICT risk management and oversight of critical third-party providers (including cloud services) in the financial sector.

Law stated - 4 May 2025

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Luxembourg saw the introduction of legal initiatives that integrate data protection. A notable example is a draft bill of law (Bill No. 8476) introduced in late 2024 to implement the EU Artificial Intelligence Act.

A landmark data protection case reached a climax in 2024/2025 involving Amazon. In 2021, the National Commission for Data Protection (CNPD) issued a record General Data Protection Regulation fine of €746 million against Amazon for unlawful personal data processing in its advertising system. Amazon's appeal was heard in January 2024, and the Luxembourg Administrative Tribunal issued its judgement on 18 March 2025, upholding the CNPD's decision in full.

The CNPD identified artificial intelligence and new technologies as a key focus. In March and April 2024, it organised DaProLab sessions on issues relating to AI. In May 2024, the CNPD launched the Sandkëscht programme, a regulatory sandbox for AI – an isolated digital environment allowing companies in Luxembourg to test AI systems for a limited time before their deployment on the market.

Law stated - 4 May 2025