

# Luxembourg Implementation of the GDPR

by **Astrid Wagner** and **Eloïse Patocki-Tomas**, Arendt & Medernach, S.A., with Practical Law Data Privacy Advisor

Practice notes | Law stated as of **24-Aug-2021** | European Union, Luxembourg

---

A Practice Note discussing the requirements of the **Luxembourg Act**, which implements the EU General Data Protection Regulation (GDPR). This Note discusses the applicability of Luxembourg data protection law and key provisions of the Luxembourg Act, such as rules for processing special categories of personal data and criminal conviction and offense data, the age of child consent, limitations on the scope of data subjects' rights, processing for journalistic purposes or artistic or literary expression, processing for archiving in the public interest, scientific or historical research, or statistical purposes, processing in the employment context, and provisions on electronic surveillance.

---

## Applicability of the GDPR and Luxembourg Law

Territorial Scope

Material Scope

## Data Protection Officers

## Processing Special Categories of Personal Data

GDPR Exceptions Permitting Processing

Luxembourg Act Exceptions That Permit Processing Special Categories of Personal Data

Genetic, Biometric, and Health-Related Data

## Processing Criminal Conviction and Offense Data

## Processing for Secondary Purposes

## Child Consent

## Data Subjects' Rights

GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights

Luxembourg Law Exceptions to Data Subject Rights

## Derogations for Specific Processing Situations

Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression

Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes

Secrecy Obligations

Processing in the Employment Context

## Other GDPR Derogations

Supervisory Authority

Administrative Fines for Public Authorities and Bodies

Additional Penalties for GDPR Violations

## Luxembourg Act and GDPR Statutory References

The [EU General Data Protection Regulation \(Regulation \(EU\) 2016/679\)](#) (GDPR) took effect on May 25, 2018, replacing the [EU Data Protection Directive \(Directive 95/46/EC\)](#) (EU Directive) and its local implementing laws. The GDPR introduced a single legal framework across the EU. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding some requirements.

Luxembourg enacted the [Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework](#) (Luxembourg Act), which aligns Luxembourg data protection law with the GDPR. The Luxembourg Act repealed the prior [Amended Act of 2 August 2002 on the protection of persons with regard to the processing of personal data](#) and amended the [Labor Code](#) (in French) and the amended [Act of 25 March 2015 stipulating the rules of remuneration and the terms and conditions for the promotion of State civil servants](#) (in French). These laws and other Luxembourg laws implementing the GDPR's provisions are outside the scope of this Note.

Luxembourg also enacted the [Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal matters and in matters of national security](#) (in French) (Law Enforcement Directive Implementing Law) to implement the [EU Law Enforcement Directive \(Directive \(EU\) 2016/680\)](#) (Law Enforcement Directive), which governs processing [personal data](#) by law enforcement authorities for the prevention, investigation, detection, and prosecution of offenses and the execution of punishments. The details of the Law Enforcement Directive and implementing law are outside the scope of this Note.

This Note discusses the Luxembourg Act's applicability and key provisions, including requirements on:

- Processing [special categories of personal data](#), including genetic data.
- Processing criminal conviction and offense data.
- Processing for secondary purposes.
- The age of child consent.
- Limiting the scope of [data subjects' rights](#) and [controllers' and processors' related obligations](#).
- Processing for journalistic purposes or academic, artistic, or literary expression.
- Processing for archiving in the public interest, scientific or historical research, or statistical purposes.
- Processing requiring authorization.
- Administrative fines and other penalties.
- Processing personal data in the employment context.
- Electronic surveillance.

For more on the GDPR's application in Luxembourg and guidance from the National Commission for Data Protection (CNPD), see [GDPR Data Protection Authority Guidance Tracker by Country \(EEA\): Luxembourg](#).

## Applicability of the GDPR and Luxembourg Law

### Territorial Scope

The GDPR applies to:

- Controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU (Article 3(1), GDPR).
- Controllers and processors not established in the EU that process personal data about data subjects in the EU when the processing activities relate to:
  - offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment; or
  - monitoring data subjects' behavior that takes place in the EU.

(Article 3(2), GDPR.)

- Controllers not established in the EU that process personal data and that are subject to EU member state law under public international law (Article 3(3), GDPR).

Some EU member states have passed national laws that include a territorial scope provision that mirrors GDPR Article 3. Other member states' laws include different applicability language or do not include a territorial scope provision. The Luxembourg Act states that the provisions of Title II apply to controllers and processors established in Luxembourg (Article 2, Luxembourg Act).

For more on the GDPR's applicability, see [Practice Note, Determining the Applicability of the GDPR](#).

### Material Scope

The GDPR includes a material scope provision stating that it applies to personal data processing wholly or partly by automated means and processing by non-automated means when the personal data forms part of or is intended to form part of a filing system (Article 2(1), GDPR). According to the GDPR, it does not apply to:

- Activities that fall outside the scope of EU law.
- Processing by EU member states under Title V, Chapter 2 of the Treaty on European Union relating to foreign and security policy.
- Processing for purely personal or household activities.
- Processing by competent authorities to prevent, investigate, detect, or prosecute criminal offenses and execute criminal penalties, including safeguarding against and preventing threats to public safety.

(Article 2(2), GDPR.)

Any personal data processing not covered by the GDPR or the Law Enforcement Directive Implementing Law is regulated by the Luxembourg Act and the GDPR provisions in:

- Article 4, Definitions.
- Chapter II, Principles.
- Chapter III, Rights of Data Subject.
- Chapter IV, Controller and Processor.
- Chapter V, Transfer of Personal Data to Third Countries or International Organisations.
- Chapter VI, Independent Supervisory Authorities.
- Chapter VII, Section 1, Cooperation.
- Chapter VIII, Remedies, Liability and Penalties.
- Chapter IX, Provisions Relating to Specific Processing Situations.

## Data Protection Officers

The GDPR requires controllers and processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). The Luxembourg Act requires controllers processing data for scientific or historical research or statistical purposes to implement certain additional measures, including appointing a data protection officer (Article 65(1), Luxembourg Act). For more on the required measures, see [Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#).

The Luxembourg Act does not bind DPOs to specific confidentiality or secrecy obligations, but DPOs generally are subject to the same professional secrecy obligations as their employer. The Luxembourg Act addresses professional secrecy obligations for lawyers, notaries, and auditors regarding the CNPD's access powers (Article 67, Luxembourg Act; see [Secrecy Obligations](#)).

Sectoral laws may also require organizations to appoint a DPO, for example, [Bill No. 7511](#) (in French) amending the [Law of 7 December 2015 on processing health-related personal data in the insurance and reinsurance sectors](#) (in French). The details of sector-specific laws are outside the scope of this note.

For more on appointing DPOs under the GDPR, see [Practice Note, Overview of EU General Data Protection Regulation: Appointment of a data protection officer](#) and [GDPR Data Protection Authority Guidance Tracker by Country \(EEA\): Luxembourg](#).

## Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR). Special categories of personal data include:

- Racial or ethnic origin.
- Political opinions.

- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health or sex life.
- Sexual orientation.

(Article 9(1), GDPR.)

## GDPR Exceptions Permitting Processing

GDPR Article 9(2) includes several exceptions to the prohibition on processing special categories of personal data. Some of these exceptions require data controllers to consult EU or member state law to determine a lawful basis for processing.

The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the controller's obligations and exercising the controller's or data subjects' rights in the fields of employment law, social security, and social protection (Article 9(2)(b), GDPR).
- Reasons of substantial public interest (Article 9(2)(g), GDPR).
- Purposes of preventive or occupational medicine, assessing an employee's working capacity, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems and services, or under a contract with a health care professional, subject to certain conditions and safeguards (Article 9(2)(h), GDPR).
- Reasons of public interest in the area of public health (Article 9(2)(i), GDPR).
- Archiving in the public interest, scientific or historical research, or statistical purposes (Article 9(2)(j), GDPR).

Other GDPR Article 9 exceptions provide a sufficient legal basis for processing special categories of personal data without the need for a further basis in EU or member state law, including when the data subject consents to processing (Article 9(2)(a), (c)-(f), GDPR).

EU or member state law may prohibit the use of data subject consent as a legal basis for processing special categories of personal data (Article 9(2)(a), GDPR). However, the Luxembourg Act does not prohibit this. Other Luxembourg laws may prohibit the use of consent as a legal basis for processing special categories of personal data in certain circumstances.

For more on processing special categories of personal data under the GDPR, see [Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data](#).

## **Luxembourg Act Exceptions That Permit Processing Special Categories of Personal Data**

The Luxembourg Act permits processing special categories of personal data for:

- Journalistic purposes or academic, artistic, or literary expression (Article 62(1), Luxembourg Act; see [Processing Special Categories of Data for Journalistic Purposes or Academic, Artistic, or Literary Expression](#)).
- Archiving in the public interest, scientific or historical research, or statistical purposes (Articles 64 and 65, Luxembourg Act; see [Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)).

All other processing relating to special categories of personal data must comply with GDPR Article 9 (see [GDPR Exceptions Permitting Processing](#)) and other applicable national laws, for example:

- [Bill No. 7511](#) (in French) amending the Law of 7 December 2015 on processing health related personal data in the insurance and reinsurance sectors.
- [Bill No. 7373](#) (in French) amending the Law of 23 December 1998 on processing personal data in the finance and insurance sectors.

Other national law requirements are outside the scope of this Note.

### **Processing Special Categories of Data for Journalistic Purposes or Academic, Artistic, or Literary Expression**

The Luxembourg Act permits processing special categories of personal data for the sole purpose of journalism or academic, artistic, or literary expression when the processing relates to personal data that:

- The data subject made public.
- Directly relates to the data subject's public life or a public activity in which the data subject voluntarily participated.

(Article 62(1), Luxembourg Act.)

### **Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes**

The Luxembourg Act permits processing special categories of personal data for archiving in the public interest, scientific or historical research, or statistical purposes if the controller implements certain additional appropriate measures, including:

- Appointing a DPO (see [Data Protection Officers](#)).
- Performing a data protection impact assessment of the planned processing activities.

- Engaging in anonymization, pseudonymization, or other operational separation measures to ensure that it cannot use the data to make decisions or take actions concerning data subjects.
- Using a trusted, independent third party to anonymize or pseudonymize the personal data.
- Encrypting personal data in transit and at rest and engaging in state-of-the-art encryption key management.
- Using technology that protects data subjects' private lives.
- Restricting access to personal data within the controller.
- Using log files that record the reason, date, and time that a person consults, collects, modifies, or deletes the personal data and the identity of the person doing so.
- Ensuring staff are aware of personal data processing and professional secrecy obligations.
- Regularly evaluating the effectiveness of the organization's technical and organizational measures through an independent audit.
- Drafting a data management plan before beginning the processing.
- Adopting applicable sector-specific codes of conduct under GDPR Article 40.

(Articles 64 and 65, Luxembourg Act.)

When deciding which additional measures to implement, controllers must:

- Consider:
  - the processing's nature, scope, context, and purposes; and
  - the likelihood and severity of the risks to data subjects' rights and freedoms.
- Document and justify not implementing any of the above measures.

(Article 65, Luxembourg Act.)

## **Genetic, Biometric, and Health-Related Data**

The GDPR permits EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR). The Luxembourg Act prohibits controllers from processing genetic data to exercise their specific rights in the labor law and insurance fields (Article 66, Luxembourg Act). It does not further limit the processing of genetic, biometric, or health-related data. However, other national laws may apply.

The Luxembourg Act exceptions that permit processing special categories of data for the following purposes also apply to genetic, biometric, and health data:

- Journalistic purposes or academic, artistic, or literary expression (see [Processing Special Categories of Data for Journalistic Purposes or Academic, Artistic, or Literary Expression](#)).

- Archiving in the public interest, scientific or historical research, or statistical purposes (see [Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)).

## Processing Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions and offenses when either:

- Carried out under the control of official authority, for example, the police.
- Authorized by EU or member state law providing for appropriate safeguards for data subjects.

(Article 10, GDPR.)

The Luxembourg Act permits processing criminal conviction and offense data for the sole purpose of journalism or academic, artistic, or literary expression when the processing relates to personal data that:

- The data subject made public.
- Directly relates to the data subject's public life or a public activity in which the data subject voluntarily participated.

(Article 62(1), Luxembourg Act.)

The [Law of 29 March 2013 on the organization of the criminal record](#), as amended by the [Law of 23 July 2016](#) (both in French) (Criminal Records Act), regulates the processing of criminal record data. For example, the Criminal Records Act only permits employers to request an individual's criminal record under certain circumstances. Controllers may also process criminal conviction and offense data where another applicable local or EU member state law requires or permits the processing. Other laws are outside the scope of this Note.

The Law Enforcement Directive Implementing Law governs public authorities' personal data processing for preventing, investigating, detecting, prosecuting, or enforcing criminal offenses or executing criminal penalties, including protecting against and preventing threats to public security. The details of this law are outside the scope of this Note.

## Processing for Secondary Purposes

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose (see [GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights](#)).

(Article 6(4), GDPR.)

Without data subject consent, any secondary processing purpose must both:

- Be compatible with the original processing purpose.
- Satisfy the conditions in GDPR Article 6(4).

(Article 6(4), GDPR.)

To determine the secondary processing purpose's compatibility, the controller should consider the criteria specified in GDPR Article 6(4) (see [Practice Note, Overview of EU General Data Protection Regulation: Further compatible processing](#)).

The Luxembourg Act does not contain provisions on secondary processing. The Law Enforcement Directive Implementing Law and other national laws may include specific provisions on processing for secondary purposes. Other laws are outside the scope of this Note.

## Child Consent

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, provided the age is not lower than 13 (Article 8(1), GDPR). The Luxembourg Act does not lower the age of child consent or otherwise change the requirements for collecting and processing children's personal data.

## Data Subjects' Rights

The GDPR grants data subjects several rights and imposes several obligations on controllers relating to those rights in Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) (see [Practice Note, Data Subject Rights Under the GDPR](#)). The GDPR permits EU member states to restrict the scope of these data subject rights and controllers' related obligations when the restriction is a necessary and proportionate measure to safeguard certain objectives or in other specific processing situations (Articles 23 and 85 to 91, GDPR; see [GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights](#) and [Derogations for Specific Processing Situations](#)).

### GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights

EU member states may restrict the scope of data subjects' rights and controllers' related obligations in GDPR Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.

- Other important economic or financial public interests of the EU or member state, including:
  - monetary, budgetary, and taxation matters;
  - public health; and
  - social security.
- Judicial independence and proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
  - national or public security;
  - defense;
  - other important public interests;
  - crime prevention; or
  - breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

EU or member state laws restricting data subjects' rights to ensure GDPR Article 23 objectives must, when relevant, include provisions on:

- Purposes of the processing or categories of processing.
- Categories of personal data.
- Scope of the restrictions.
- Safeguards to prevent abuse or unlawful access or transfer.
- Specification of the controller or categories of controllers.
- Data retention periods and applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- Risks to the rights and freedoms of data subjects.
- Data subjects' rights to be informed about restrictions, unless doing so is prejudicial to the restriction's purpose.

(Article 23(2), GDPR.)

## Luxembourg Law Exceptions to Data Subject Rights

The Luxembourg Act does not introduce any exceptions to data subject rights based on GDPR Article 23 objectives, but it includes provisions limiting certain data subject rights when processing personal data for:

- Journalistic purposes or academic, artistic, or literary expression (Article 62(3), (4), Luxembourg Act; see [Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression](#)).
- Scientific or historical research or statistical purposes (Article 63, Luxembourg Act; see [Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)).

Other national laws may also limit certain data subject rights, such as:

- Bill No. 7511 (in French) amending the Law of 7 December 2015 on processing health related personal data in the insurance and reinsurance sectors.
- Bill No. 7373 (in French) amending the Law of 23 December 1998 on processing personal data in the finance and insurance sectors.

Other national laws are outside the scope of this Note.

## Derogations for Specific Processing Situations

GDPR Articles 85 to 91 provide additional rules that apply to seven specific processing situations (Articles 85 to 91). These Articles permit EU member states to enact further rules that apply to the specified processing types. The Luxembourg Act introduces further rules that apply to:

- Processing for journalistic purposes or academic, artistic, or literary expression (see [Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression](#)).
- Processing for archiving in the public interest, scientific or historical research, or statistical purposes (see [Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)).
- Secrecy obligations (see [Secrecy Obligations](#)).
- Processing in the employment context (see [Processing in the Employment Context](#)).

## Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression

The GDPR permits EU member states to establish derogations from the GDPR when necessary to reconcile the right to personal data protection with the right to freedom of expression and information, including when processing for journalistic purposes or for academic, artistic, or literary expression (Article 85, GDPR). Certain GDPR provisions do not apply when processing personal data solely for journalism or academic, artistic, or literary expression, including:

- The prohibition on processing special categories of personal data under GDPR Article 9(1) and the limitations on processing criminal conviction and offense data under GDPR Article 10 when the processing relates to personal data that:

- the data subject made public; or
- directly relates to the data subject's public life or public activities in which they voluntarily participated.
- The requirements on transferring personal data to third countries or international organizations under GDPR Chapter V (Article 62(2), Luxembourg Act).
- The obligations under GDPR Article 13 to provide information to data subjects when providing the information would compromise data collection from the data subject.
- The obligations under GDPR Article 14 to provide information to data subjects when providing the information would:
  - compromise data collection;
  - compromise planned publication or otherwise making the data available to the public in any manner; or
  - identify information sources.

Controllers may also limit data subjects' access rights when processing for these purposes. Information provided by controllers should not include information on the origin of data or allowing for identification of the data's source. (Article 62, Luxembourg Act.)

## **Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes**

The GDPR permits EU member states to establish rules when processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes (Article 89, GDPR). The Luxembourg Act permits processing personal data (including special categories of personal data) for archiving in the public interest, scientific or historical research, or statistical purposes if the controller implements the additional measures set out in Luxembourg Act Article 65 (Article 64, Luxembourg Act; see [Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)). For more on processing special categories of personal data, see [Processing Special Categories of Personal Data](#).

Controllers processing personal data for scientific or historical research or statistical purposes may restrict data subjects' access (Article 15, GDPR), rectification (Article 16, GDPR), processing restriction (Article 18, GDPR), and objection (Article 21, GDPR) rights if:

- Exercising those rights likely renders impossible or seriously impairs achieving the processing purposes.
- The controller implements the security requirements set out in Luxembourg Act Article 65 (see [Processing Special Categories of Data for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes](#)).

(Article 63, Luxembourg Act.)

## **Secrecy Obligations**

The GDPR permits EU member states to adopt rules specifying the powers of [supervisory authorities](#) regarding controllers and processors that are subject to:

- An obligation of professional secrecy.
- Another equivalent secrecy obligation.

(Article 90, GDPR.)

The Luxembourg Act provides the CNPD with the investigative powers set out in GDPR Article 58(1) (Article 12, Luxembourg Act). When the CNPD exercises its access powers under GDPR Article 58(1)(e) and (f) against:

- Lawyers, the access must comply with Article 35, paragraph 3 of the amended [Act of 10 August 1991 on the legal profession](#) (in French).
- Notaries, the access must comply with Article 41 of the amended [Act of 9 December 1976 on the notarial profession](#) (in French).
- Auditing professionals, the access must comply with Article 28, paragraph 8 of the amended [Act of 23 July 2016 on the auditing profession](#) (in French).

(Article 67(1)-(3), Luxembourg Act.)

These requirements only apply to personal data that the lawyer, notary, or auditing professional obtained in the course of activities subject to professional secrecy obligations (Article 67(4), Luxembourg Act).

## **Processing in the Employment Context**

The GDPR permits EU member states to provide more specific rules, by law or collective agreements, on the processing of personal data in the employment context (Article 88, GDPR). The Luxembourg Act applies in the employment context generally. However, it also amends the Labor Code to add rules on employee surveillance (see [Electronic Surveillance](#)). The Luxembourg Act also prohibits controllers from processing genetic data for the purpose of exercising their rights under labor law (Article 66, Luxembourg Act; see [Genetic, Biometric, and Health-Related Data](#)).

Employers should use caution when relying on consent in the employment context. EU supervisory authorities generally consider consent given in the employment context to be not freely given and therefore invalid. Consent must comply with GDPR Articles 7 (Conditions for consent) and 6(1)(a), which require data subjects to give consent for specified purposes. For more on relying on employee consent under the GDPR, see [Practice Note, Employee Consent Under the GDPR](#).

### **Electronic Surveillance**

The Luxembourg Act amends the Labor Code, adding provisions on employee surveillance that require employers to:

- Meet one of the legal bases for processing personal data set out in GDPR Article 6(1)(a) to (f) (see [Practice Note, Overview of EU General Data Protection Regulation: Lawfulness of processing](#)).
- Before beginning employee surveillance, provide certain employees with a notice containing:

- the processing purpose;
- the implementing measures for the surveillance system;
- the length and criteria for data retention, if necessary; and
- a formal commitment that the employer will not use the data collected for any purpose other than the processing purpose set out in the notice.

(Article 71, Luxembourg Act (amending Labor Code Article L.261-1(1)-(2)).)

The Luxembourg Act grants employees the rights to:

- Submit a request to the CNPD for an opinion on the compliance of the planned employee surveillance within 15 days of the employer's notice under Labor Code Article L.261-1(2). The CNPD must respond within 30 days, and the employer cannot begin the employee surveillance while the request is pending.
- Lodge a complaint to the CNPD, which the employer cannot use as a serious or legitimate cause for an employee's dismissal.

(Article 71, Luxembourg Act (amending Labor Code Article L.261-1(4)-(5)).)

Additional requirements apply to employers under Labor Code Articles L.211-8, L.414-9, and L.423-1 if they process the data collected through surveillance:

- For employee health and safety.
- To monitor employees' output or services when this is the only way to determine their exact salary.
- Within the framework of a flexi-time work organization under the Labor Code.

(Article 71, Luxembourg Act (amending Labor Code Article L.261-1(3)).)

## Other GDPR Derogations

### Supervisory Authority

GDPR Article 54 requires each EU member state to establish a supervisory authority. Articles 16 to 27 of the Luxembourg Act set out the structure, organization, tasks, and powers of the CNPD. The CNPD consists of four members, including a chairperson (Article 16, Luxembourg Act).

The CNPD has the tasks and powers specified in GDPR Articles 57 and 58 (Articles 7 and 12, Luxembourg Act). The Luxembourg Act assigns the CNPD additional tasks and powers, such as:

- Monitoring and enforcing the Law Enforcement Directive Implementing Law (Article 8, Luxembourg Act).
- Publishing an annual report of GDPR and Law Enforcement Directive Implementing Law violations and the punishments imposed (Article 10, Luxembourg Act).

- Investigating and deciding alleged violations of the GDPR and the Law Enforcement Directive Implementing Law (Articles 37 to 41, Luxembourg Act).
- Issuing sanctions for violations of the GDPR and Law Enforcement Directive Implementing Law (Articles 48 to 52, Luxembourg Act).

## Administrative Fines for Public Authorities and Bodies

The GDPR permits EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies (Article 83(7), GDPR). The Luxembourg Act prohibits the CNPD from imposing administrative fines on state and municipal authorities (Article 48, Luxembourg Act).

## Additional Penalties for GDPR Violations

The GDPR permits EU member states to specify penalties for GDPR violations that are not subject to administrative fines under GDPR Article 83 (Article 84, GDPR). The Luxembourg Act authorizes the CNPD to impose:

- Criminal sanctions against anyone who prevents or hinders its mission, including:
  - imprisonment from eight days to one year; or
  - a fine between EUR251 and EUR125,000.

(Article 51, Luxembourg Act.)

- Periodic penalties of up to 5% of the controller's or processor's average daily turnover during the previous financial year to compel them to:
  - communicate all information the CNPD requests under GDPR Article 58(1)(a); or
  - comply with a corrective measure the CNPD adopts under GDPR Article 58(2)(c)-(h) and (j).

(Article 49(1), Luxembourg Act.)

### Luxembourg Act and GDPR Statutory References

Subject Matter	Luxembourg Act Section	GDPR Article Permitting Member State Derogation
Applicability of Luxembourg law (see <a href="#">Applicability of the GDPR and Luxembourg Law</a> )	1, 2	N/A
Appointing a data protection officer (see <a href="#">Data Protection Officers</a> )	65	37(4), 38(5)
Processing special categories of personal data (see <a href="#">Processing</a> )	62, 64, 65	9(2)

<b>Special Categories of Personal Data</b>		
Genetic, biometric, and health-related data (see <a href="#">Genetic, Biometric, and Health-Related Data</a> )	66	9(4)
Processing criminal conviction and offense data (see <a href="#">Processing Criminal Conviction and Offense Data</a> )	62	10
Processing for secondary purposes (see <a href="#">Processing for Secondary Purposes</a> )	N/A	6(4)
Child consent (see <a href="#">Child Consent</a> )	N/A	8(1)
Limitations on data subjects' rights (see <a href="#">Data Subjects' Rights</a> )	62, 63	23, 85 to 91
Processing for journalistic purposes or academic, artistic, or literary expression (see <a href="#">Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression</a> )	62	85
Processing for archiving in the public interest, scientific or historical research, or statistical purposes (see <a href="#">Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes</a> )	63	89
Secrecy Obligations (see <a href="#">Secrecy Obligations</a> )	67	90
Processing employee personal data (see <a href="#">Processing in the Employment Context</a> )	14	88
Using electronic surveillance (see <a href="#">Electronic Surveillance</a> )	71	6(1)(c), (e)
Supervisory authority (see <a href="#">Supervisory Authority</a> )	Chapter II	51, 54
Administrative fines for public authorities and bodies (see <a href="#">Administrative Fines for Public Authorities and Bodies</a> )	48	83(7)
Additional penalties for GDPR violations (see <a href="#">Additional Penalties for GDPR Violations</a> )	51, 49	84

END OF DOCUMENT