TABLE OF CONTENTS

September 2023

1. Governing Texts

Since the entry into force of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which repealed the Data Protection Directive (Directive 95/46/EC), data protection in Luxembourg has been governed primarily by the GDPR and, on a subsidiary basis, by Act of August 1, 2018, on the Organization of the National Commission for Data Protection and Implementing the GDPR ('the Act') which contains very limited derogations to the GDPR. The purpose of the Act is essentially to complement the GDPR and to define the roles and responsibilities of the National Commission for Data Protection ('CNPD') which is tasked with overseeing and enforcing the GDPR.

Since the constitutional reform, which entered into force on July 1, 2023, data protection has been raised to a constitutional level in Luxembourg.

In addition to the Act, there are a certain number of separate and specific pieces of legislation that deal with aspects of data protection, but in this case, data protection is treated as ancillary.

1.1. Key acts, regulations, directives, bills

The main laws with respect to data protection and privacy in Luxembourg are:

- The Act. Such a law formally repeals the previous law on data protection and implements the GDPR at the national level while introducing certain limited derogations.
- The Act of August 1, 2018, on the Protection of Individuals with regard to the Processing of Personal Data in Criminal and National Security Matters (only available in French here) ('the 'Law on National Security Matters') which transposes into national law Directive (EU) 2016/680 of April 27, 2016.

Act of May 30, 2005, Laying Down Specific Provisions for the Protection of Persons with regard to the Processing of Personal Data in the Electronic Communications Sector and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure, as amended (only available in French here) ('the Electronic Communications Act'), which transposes Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive') into national law. It regulates the protection of personal data in the field of telecommunications and electronic communications and takes into account recent and foreseeable developments in the field of electronic communications services and technologies.

There are several Grand-Ducal Regulations relating to data protection such as:

- the Grand-Ducal Regulation of October 8, 2020, establishing the seat of the CNPD (only available in French here);
- the Grand-Ducal Regulation of August 1, 2018, setting the allowances payable to the President, members of the College and alternate members of the CNPD (only available in French here); and
- the Grand-Ducal Regulation of July 24, 2010, determining the categories of personal data generated or processed in connection with the provision of electronic communications services or public communications networks (only available in French here).

Apart from the above, there are numerous laws and regulations regulating specific sectors and containing some data protection and privacy-related aspects, including, for example, the following:

- **in relation to data processing by police authorities:** the Grand-Ducal regulation of July 22, 2008, implementing article 48-24 of the Code of Criminal Procedure and article 34-1 of

the amended law of May 31, 1999, on the Police and the Inspectorate-General of the Police (only available in French here) which defines how authorities may access the common register of natural and judiciary persons as well as databases from the 'Centre commun de la Sécurité sociale' in the context of asylum-seekers, visa-requests, business licences, driving licences, taxes, and firearms licences;

- **in relation to data processing by health services:** the Grand-Ducal Regulation of April 18, 2013, determining the terms and conditions of operation of the national cancer register and amending the Grand-Ducal Regulation of June 20, 1963, making it compulsory to declare the causes of death (only available in French here) which sets up a national cancer register purported to collect data relating to cancer pathologies and implemented for public health and research purposes;
- **in relation to the fight against money laundering and terrorist financing:** the law of January 13, 2019, creating a Register of beneficial owners, as amended (only available in French here) and the Grand-Ducal Regulation of February 15, 2019, on the arrangements regarding registration and payment of administrative costs as well as the access to the information registered in the Register of beneficial owners (only available in French here), which relate to the creation and management of a beneficial ownership register aimed at identifying, for transparency purposes, the natural person(s) who ultimately own(s) or control(s) the undertaking being the clients of professionals and/or the natural person(s) on whose behalf a transaction or activity is carried out; and
- **in relation to whistleblowing:** the law of May 16, 2023, transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law (only available in French here).

1.2. Guidelines

The CNPD is the supervisory authority within the meaning of Article 51 of the GDPR and is responsible for monitoring the application of the GDPR.

The CNPD has issued various guidelines and fact sheets over the last few years. Among these guidelines, the most notable are those relating to:

- cookies and other tracking devices (only available in French here);
- geolocation of vehicles made available to employees (only available in French here);
- video surveillance (only available in French here);
- image rights (only available in French here);
- data protection rules for social elections (only available in French here); and

- election campaigns in compliance with the protection of personal data (only available in French here).

Aside from those guidelines, the CNPD also makes available on its website certain more general guidance for both data subjects and professionals.

In addition to the CNPD, there are a number of other authorities, professional associations and orders that provide their members with guidance on GDPR compliance.

1.3. Case law

There is at this stage limited public case law available involving specifically breaches and/or interpretations of the GDPR.

The most notable judicial decisions on the GDPR to date are certainly the decisions of the Luxembourg District Court rendered on November 13, 2020, (ref. 2020TALCH02/01568) and on January 24, 2020, as they gave rise to two requests for preliminary rulings (joined cases C-37/20 *WM and Luxembourg Business Registers* and C-601/20 *Sovim SA and Luxembourg Business Registers*) on the interpretation of certain provisions of the Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015, ('the 4th AML Directive'), as amended by the Directive 2018/84. Such requests for preliminary rulings are at the origin of the decision of the Court of Justice of the European Union of November 22, 2022, which ruled that the provision of the amended 4th AML Directive requiring Member States to ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory be accessible in all cases to any member of the general public, was invalid.

Decisions of the CNPD which do not have the character of jurisprudence *per se* are discussed in the section below on penalties.

2. Scope of Application

2.1. Personal scope

There are no national law variations on this aspect so the provisions of the GDPR fully apply.

2.2. Territorial scope

There are no national law variations on this aspect so the provisions of the GDPR fully apply.

2.3. Material scope

There are no national law variations on this aspect so the provisions of the GDPR fully apply.

3. Data Protection Authority | Regulatory Authority

3.1. Main regulator for data protection

The main and sole regulator for data protection and supervisory authority within the meaning of Article 51 of the GDPR is the CNPD.

3.2. Main powers, duties and responsibilities

The CNPD's mission and responsibilities remain identical to those set out in Article 57 of the GDPR.

The CNPD has been vested with all the powers of investigation, powers of correction, powers of authorization and powers of consultation conferred by Article 58 of the GDPR on the supervisory authorities.

Investigative powers:

- to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- to carry out investigations in the form of data protection audits;
- to carry out a review of certifications issued pursuant to Article 42(7) of the GDPR;
- to notify the controller or the processor of an alleged infringement of the GDPR;
- to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; and
- to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Corrective powers

- to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of the GDPR;
- to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR;
- to order the controller or the processor to comply with the data subject's requests to exercise their rights pursuant to the GDPR;
- to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- to order the controller to communicate a personal data breach to the data subject;
- to impose a temporary or definitive limitation including a ban on processing;
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17, and 18 of the GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Articles 17(2) and 19 of the GDPR;
- to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 of the GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- to impose an administrative fine pursuant to Article 83 of the GDPR, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; and
- to order the suspension of data flows to a recipient in a third country or to an international organization.

Authorization and advisory powers:

- to advise controllers in accordance with the prior consultation procedure referred to in Article 36 of the GDPR;
- to issue, on its own initiative or upon request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- to authorize processing referred to in Article 36(5) of the GDPR, if the law of the Member State requires such prior authorization;
- to issue an opinion and approve draft codes of conduct pursuant to Article 40(5) of the GDPR;
- to accredit certification bodies pursuant to Article 43 of the GDPR;

- to issue certifications and approve criteria of certification in accordance with Article 42(5) of the GDPR;
- to adopt standard data protection clauses referred to in Articles 28(8) and 46(2)(d) of the GDPR;
- to authorize contractual clauses referred to in Article 46(3)(a) of the GDPR;
- to authorize administrative arrangements referred to in Article 46(3)(b) of the GDPR; and
- to approve binding corporate rules pursuant to Article 47 of the GDPR.

4. Key Definitions

Data controller: No national variations from the GDPR.

Data processor: No national variations from the GDPR.

Personal data: No national variations from the GDPR.

Sensitive data: No national variations from the GDPR.

Health data: No national variations from the GDPR.

Biometric data: No national variations from the GDPR.

Pseudonymization: No national variations from the GDPR.

5. Legal Bases

5.1. Consent

No national variations from the GDPR.

5.2. Contract with the data subject

No national variations from the GDPR.

5.3. Legal obligations

No national variations from the GDPR.

5.4. Interests of the data subject

No national variations from the GDPR.

5.5. Public interest

No national variations from the GDPR.

5.6. Legitimate interests of the data controller

No national variations from the GDPR.

5.7. Legal bases in other instances

No national variations from the GDPR.

6. Principles

No national variations from the GDPR.

7. Controller and Processor Obligations

7.1. Data processing notification

Luxembourg does not have a data processing registration requirement.

7.2. Data transfers

No national variations from the GDPR.

7.3. Data processing records

No national variations from the GDPR.

7.4. Data protection impact assessment

The CNPD adopted on March 11, 2019, a list of processing operations for which a Data Protection Impact Assessment ('DPIA') is mandatory in accordance with Article 35(4) of the GDPR.

The list adopted by the CNPD was submitted to the European Data Protection Supervisor (the 'EDPS') to ensure consistency and uniformity in the application of the GDPR at the European level but such a list is not exhaustive and the CNPD states that there may remain a need to carry-out DPIAs in circumstances not mentioned in this list. The said list is limited to processing activities that will always require a DPIA to be carried out. The CNPD's list entails:

- processing operations involving genetic data as defined in Article 4(13) of the GDPR, in combination with at least one other criterion in the guidelines of the EDPS, with the exception of healthcare professionals providing healthcare services;
- processing operations that include biometric data as defined in Article 4(14) of the GDPR for the purpose of identifying data subjects in combination with at least one other criterion in the EDPS guidelines;
- processing operations involving the combination, matching or comparison of personal data collected from processing operations with different purposes (originating from the same or different controllers) - provided that they produce legal effects with respect to the natural person or have a significant and similar impact on the natural person;
- processing operations that consist of or include regular and systematic monitoring of employees' activities - provided that they may produce legal effects with regard to the employees or affect them in a similarly significant manner;
- processing operations relating to files which are likely to contain the personal data of the entire national population provided that such a DPIA has not already been carried out as part of a general impact assessment in the context of the adoption of this legal basis;
- processing operations for scientific or historical research purposes, or for statistical purposes within the meaning of Articles 63 to 65 of the Act;
- processing operations that consist of systematically tracking the whereabouts of natural persons; and
- processing operations based on the indirect collection of personal data in conjunction with at least one other criterion of the EDPS guidelines where it is neither possible nor feasible to guarantee the right to information.

7.5. Data protection officer appointment

There are no national variations on this aspect and the GDPR fully applies.

A data protection officer ('DPO') has however to be appointed by controllers, according to Article 65 of the Act, for processing carried out for scientific, historical research, or statistical purposes taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

If they appoint a DPO (on a mandatory or elective basis), data controllers and processors are obliged to communicate the contact details of the DPO to the CNPD. The CNPD has provided a specific form on its website for this purpose.

7.6. Data breach notification

There are no national variations on this aspect and the GDPR fully applies. Specific forms have been made available by the CNPD, on its website, for the purpose of such notifications.

7.7. Data retention

The Act does not contain any retention periods or other timeframes. However, there are many sector-specific laws that contain references to minimum statutory retention periods and possible extensions, which may be taken into account when assessing retention periods.

7.8. Children's data

No national variations from the GDPR.

7.9. Special categories of personal data

There are multiple sector-specific laws containing provisions regarding the processing of special categories of personal data, including criminal conviction data (e.g. the Law on National Security Matters). Such laws however do not deviate from the principles set out under Article 9 of the GDPR.

The Act expressly provides that the processing of special categories of data is not subject to the prohibition set out in Article 9(1) of the GDPR where:

- carried out for the sole purpose of journalism or academic, artistic, or literary expression when the processing relates to data manifestly made public by the data subject or to data in direct relation to the public life of the data subject or with the events in which they were voluntarily involved (Article 62(1) of the Act); and
- such processing is for scientific, historical research, or statistical purposes, as per 9(2)(j) of the GDPR and the controller meets the conditions laid down by Article 65 of the Act (Article 64 of the Act).

The Act expressly prohibits the processing of genetic data for the purpose of exercising the specific rights of the controller in the field of labour law and insurance.

7.10. Controller and processor contracts

The obligations of controllers and processors in Luxembourg are generally those set out in the GDPR. There are no national derogations or variations.

8. Data Subject Rights

8.1. Right to be informed

No national variations from the GDPR.

8.2. Right to access

No national variations from the GDPR.

8.3. Right to rectification

No national variations from the GDPR.

8.4. Right to erasure

No national variations from the GDPR.

8.5. Right to object/opt-out

No national variations from the GDPR.

8.6. Right to data portability

No national variations from the GDPR.

8.7. Right not to be subject to automated decision-making

No national variations from the GDPR.

8.8. Other rights

The right to restriction of processing; however, there are no national variations from the GDPR.

9. Penalties

The sanctions provided for in the GDPR are fully applicable to Luxembourg. However, the Act also empowers the CNPD to impose additional sanctions, such as:

- periodic penalty payments, on the controller or processor, not exceeding 5% of the average daily turnover of the preceding business year, or of the last ended business year, per day calculated from the date appointed by the decision, in order to compel such controller or processor:
    - to communicate all information required by the CNPD pursuant to Article 58(1)(a) of the GDPR; or
    - to comply with a corrective measure that the CNPD has adopted in accordance with Article 58(2)(c), (d), (e), (f), (g), (h) and (j) of the GDPR;
- sentence to imprisonment for a period of eight days to one year and a fine ranging from €251 to €125,000 or one of these punishments alone against any person who would wilfully prevent or impede, in any way, the execution of the tasks of the CNPD; and
- the complete or partial publication of its decisions, at the expense of the person sanctioned, excluding decisions relating to the imposition of periodic penalty payments, on the condition that all means of appeal against the decision have been exhausted and the publication does not risk causing disproportionate damage to the parties concerned.

The Act however provides that the CNPD may not impose the administrative fines as set out in Article 83 of the GDPR and the periodic penalty payments against the State and municipalities.

9.1 Enforcement decisions

According to the report on the activities of the CNPD for 2021 (only available in French here), the CNPD took a total of 48 decisions related to national cases, with administrative fines totalling €319,500. One decision was taken by the CNPD in the context of European cooperation against Amazon Europe Core S.à r.l., resulting in an administrative fine of €746 million. Given that the CNPD is bound by professional secrecy under the Act, the CNPD has not publicly disclosed the exact grounds on which such an administrative fine was imposed on Amazon Europe Core S.à r.l. Such fine is however at this stage the highest fine pronounced by the CNPD.