Data protection in Luxembourg: overview

by *Anne Morel*, Bonn Steichen & Partners

Country Q&A | Law stated as at 01-Jan-2019 | Luxembourg

A Q&A guide to data protection in Luxembourg.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data protection *Country Q&A tool*.

This article is part of the global guide to data protection. For a full list of contents, please visit *www.practicallaw.com/dataprotection-guide*.

Regulation

Legislation

1. What national laws regulate the collection and use of personal data?

General laws
Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)) is fully and directly applicable in Luxembourg from 25 May 2018.

The Law of 1 August 2018 came into force on 20 August 2018, adapting the national legal framework to the GDPR provisions and repealing the former Luxembourg Law of 2 August 2002 on the protection of persons with regard to the processing of personal data.

Sectoral laws
Articles L.261-1 and L.261-2 of the Labour Code specifically regulate the processing operations for workplace supervision purposes. These articles have been amended by the Law of 1 August 2018.

Scope of legislation

2. To whom do the laws apply?

The GDPR applies to the processing of personal data by:

- An establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU.
- A controller or processor not established in the EU, if the data subjects are in the EU and the processing activities are related to:
    - the offering of goods or services to the data subjects in the EU, irrespective of whether payment by the data subject is required; or
    - the monitoring of data subjects' behaviour as far as their behaviour takes place within the EU.
- A controller not established in the EU, but in a place where member state law applies by virtue of public international law.

3. What data is regulated?

The GDPR applies to the processing of personal data of natural persons.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be directly or indirectly identified, in particular by reference to an identifier such as:

- A name.
- An identification number.
- Location data.
- An online identifier.
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data that has undergone pseudonymisation, but which could be attributed to a natural person by the use of additional information, is considered to be information relating to an identifiable natural person.

The GDPR defines "pseudonymisation" as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

In addition, the GDPR specifically regulates the processing of:

- Certain categories of sensitive data. This refers to data on:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - health, sex life or sexual orientation. Personal data concerning health includes all data relating to the health status of a data subject, including information relating to their past, current or future physical or mental health status;
  - genetic data. Genetic data is defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained;
  - biometric data.
- Legal data. This includes data necessary for criminal investigations and legal proceedings and data relating to offences, criminal convictions or security measures.

4. What acts are regulated?

- The GDPR applies to processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data that forms or is intended to form part of a filing system.

The GDPR defines the processing of personal data as any operation or set of operations performed with respect to personal data, whether or not by automatic means, including:

- Collection and recording.
- Organisation, structuring and storage.
- Adaptation or alteration.
- Retrieval, consultation and use.

- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure or destruction.

5. What is the jurisdictional scope of the rules?

See *Question 2*.

6. What are the main exemptions (if any)?

The GDPR does not apply to the processing of personal data:

- In the course of an activity that falls outside the scope of EU law.
- By EU member states when carrying out activities that fall within the scope of specific provisions on the EU common foreign and security policy under the Treaty on the Functioning of the European Union (TFEU).
- By a natural person in the course of a purely personal or household activity.
- By the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security.

Notification

7. Is notification or registration required before processing data?

The GDPR does not require notifications or registrations before processing data, as it is based on a compliance system. The controller must be compliant with the applicable rules and principles.

Main data protection rules and principles

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Data controllers must respect certain principles before and during the data processing:

- **Lawfulness.** The processing must be based on one of the following grounds:
  - the data subject has given consent to the processing of their personal data for one or more specific purposes;
  - the processing is necessary for a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
  - the processing is necessary for compliance with a legal obligation to which the controller is subject;
  - the processing is necessary to protect the vital interests of the data subject or of another natural person;
  - the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
  - the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.
- **Fairness.** The data must be processed in good faith, and with the knowledge of the person whose data is concerned. The data must be erased or made anonymous as soon as possible, so that it is not used for purposes other than those originally intended. The principle of trustworthiness typically refers to the way in which data is collected.
- **Transparency.** A natural or legal person that wishes to process personal data must inform the data subject as soon as data is collected and/or when the data is passed on to third parties. This principle requires any information and communication relating to the processing of the personal data to be easily accessible and easy to understand, using clear and plain language.
- **Purpose limitation.** Personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, or for scientific or historical research or statistical purposes is not considered to be incompatible with such initial purposes.
- **Data minimisation.** The controller must only collect adequate and relevant data, and not more than is necessary to achieve the purposes of the processing.

- **Accuracy.** Incorrect or incomplete information can harm the person to whom it relates. Therefore, the data processed must be correct and up-to-date, or if not, it must be updated. Incorrect data must be corrected or deleted.
- **Storage limitation.** Personal data must not be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed. Personal data can be stored for longer periods if the personal data is processed solely for archiving purposes in the public interest, or for scientific or historical research or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of the data subject.
- **Integrity and confidentiality.** Personal data must be treated confidentially and stored in a safe place. The data processor is liable for non-compliance. This obligation persists even if the data processor has entered into a contract with a subcontractor.
- **Accountability.** The controller is responsible for, and must be able to demonstrate compliance with, all the data protection principles above.

Sensitive data is subject to enhanced protection, and in principle its processing is prohibited (see *Question 11*).

9. Is the consent of data subjects required before processing personal data?

Personal data processing must be legitimate. Consent of the data subject is one of the legal bases that can legitimise processing operations. However, the consent of a data subject employee cannot provide legitimacy for processing implemented by an employer for the purposes of supervision at a workplace, due to the relationship of subordination between the parties. An employer would therefore have to rely on one of the other grounds justifying processing under the GDPR (*see Question 10*).

The consent of the data subject is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

Consent must not be implied or inferred. It must be express, but the form in which it can be given is not the subject to in-depth regulation. The data subject has the right to withdraw their consent at any time. A withdrawal does not retroactively affect the lawfulness of prior processing.

The data subject must be informed of the processing proposed before giving consent. It must be as easy to withdraw consent as to give consent.

10. If consent is not given, on what other grounds (if any) can processing be justified?

Data processing can also be justified if it is necessary for:

- The performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.
- Compliance with a legal obligation to which the controller is subject.
- The protection of the vital interests of the data subject or of another natural person.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection, in particular where the data subject is a child.

The Law of 1 August 2018 has amended the provisions relating to justification for processing for the purposes of supervision at the workplace. According to Article L. 261-1 of the Labour Code as amended, employers must meet the GDPR justifications set out above.

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

- The processing of sensitive data (*see Question 3*) is in principle prohibited. However, the prohibition does not apply if one of the following applies:
- The data subject has given explicit consent to the processing of the personal data for one or more specified purposes.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or member state law or a collective agreement under member state law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and:
    - the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes; and

    - the personal data is not disclosed outside that body without the consent of the data subjects.

- Processing relates to personal data that is clearly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary on the basis of EU or member state law or pursuant to a contract with a health professional for the purposes of:
    - preventive or occupational medicine;
    - the assessment of the working capacity of an employee;
    - medical diagnosis;
    - provision of health or social care or treatment;
    - management of health or social care systems and services.

- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving purposes in the public interest, or for scientific or historical research or statistical purposes.
- Processing of personal data relating to criminal convictions and offences or related security measures (legal data) based on Article 6(1) of the GDPR can only be carried out under the control of official authority or when the processing is authorised by EU or member state law providing for appropriate safeguards for the rights and freedoms of data subjects.

The processing of data for supervision purposes at the workplace is subject to additional legal requirements if the processing is based on the requirement to:

- Ensure the compliance of health and safety provisions;
- Monitor on a temporary basis the production process or employees' performance to the extent that such supervision is required to determine the employees' remuneration; or
- Implement and monitor a flexible-time arrangement.

The following additional requirements apply in relation to the processing of data for supervision purposes at the workplace:

- The employer must comply with a prior information requirement on an individual basis and also on a collective basis to the concerned employees, or the staff delegation, or the Inspectorate of Labour and Mines (*Inspection du Travail et des Mines*). This is notwithstanding the right to information to the concerned employees as provided for by general data protection legal provisions (information requirement on an individual basis).
- The implementation of a flexible-time arrangement requires that the following are agreed in relation to the arrangement:
    - its period;
    - its content, terms and conditions; and

    - modification (in a collective bargaining agreement, company agreement, any inter-professional agreement on social dialogue or by common consent of the employer and the staff delegation/ employees).

- The co-decision process with the staff delegation must be complied with.
- The employees can refer the matter to the CNPD for preliminary opinion as to the compliance of the contemplated supervision measures within 15 days of receiving the prior information. The CNPD must issue an advice within one month.
- The employees' consent does not render the processing lawful.

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

If data is collected directly from the data subject, the controller must supply the data subject with the following information, unless the data subject has already been informed, no later than the point at which the data is collected and regardless of the medium of collection:

- The identity and the contact details of the controller and of its representative, if any.
- The contact details of the data protection officer (DPO), if applicable.
- The purpose or purposes of the intended data processing, as well as the legal basis for the processing.
- If the processing is based on the protection of the legitimate interests pursued by the controller or by a third party, the controller must specify those interests.
- The recipients or categories of recipients of the personal data, if any.
- If the controller intends to transfer personal data to a third country or international organisation, the existence or absence of an adequacy decision by the European Commission, and reference to the appropriate safeguards, if applicable

Further information must be provided to ensure fair and transparent processing:

- The period for which the personal data will be stored, or, if not known, the criteria used to determine that period.
- The data subject's rights to:
    - request access to and rectification or erasure of personal data;
    - restrict or object to the processing; and

    - data portability.

- When the processing is based on the data subject's consent, the existence of the right to withdraw that consent at any time without affecting the lawfulness of processing based on consent before that withdrawal.
- The right to lodge a complaint with a supervisory authority.
- Whether the provision of the data is a statutory or contractual requirement and whether the data subject must provide the personal data. The controller must inform the data subject of the possible consequences of providing the requested data.
- The existence of automated decision-making, including profiling.

If the data has not been obtained from the data subject, the controller must provide the data subject with the following information:

- The identity and the contact details of the controller and of its representative, if any.
- The contact details of the data protection officer, if applicable.
- The purpose or purposes of the processing for which the data is intended as well as the legal basis for the processing.
- The recipients or categories of recipients of the personal data, if any.
- Whether the controller intends to transfer personal data to a third country or international organisation, and the existence or absence of an adequacy decision by the European Commission and reference to the appropriate safeguards, if applicable.

Further information must be provided to ensure fair and transparent processing, such as:

- The period for which the personal data will be stored or if not known, the criteria used to determine that period.
- The data subject's rights to:
    - request access to and rectification or erasure of personal data;
    - restrict or object to the processing; and
    - data portability.

- When the processing is based on the data subject's consent, the right to withdraw that consent at any time.
- The right to lodge a complaint with a supervisory authority.

The disclosure must in principle take place at the time of undertaking the recording of personal data, but at the latest within one month of doing so, having regard to the specific circumstances in which the personal data is processed. If a disclosure to a third party is envisaged, the disclosure must be no later than the time when the data is first disclosed to that party, unless the data subject already has the information.

The data subject's right to information is not applicable to certain types of processing operations such as where:

- The provision of the information is impossible or would involve a disproportionate effort.

- Obtaining disclosure is expressly covered by EU or member state law to which the controller is subject and that protects the data subject's legitimate interests.
- The personal data must remain confidential due to an obligation of professional secrecy.

13. What other specific rights are granted to data subjects?

Data subjects have specific rights to:

- **Access.** On application to the controller, data subjects or their beneficiaries who can prove a legitimate interest have a right of access to the personal data. This right includes a confirmation as to whether data relating to them is being processed, and to receive information as to the:
  - purpose or purposes of the processing;
  - categories of data concerned;
  - recipients or categories of recipients to whom the data is disclosed; and
  - envisaged period for which the personal data will be stored or, if not known, the criteria used to determine that period.

  If the personal data is transferred to a third country, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

  The controller must provide the data subject with a copy of the personal data undergoing processing. as long as this does not affect the rights and freedoms of others.
- **Rectification.** Data subjects have the right to obtain the rectification of inaccurate personal data concerning them from the controller without undue delay.
- **Erasure.** *See Question 14.*
- **Restriction of processing.** The data subject has the right to restrict the processing, under certain conditions.
- **Data portability.** Data subjects have the right to receive the personal data concerning them that they have provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit that data to another controller. If it is technically feasible, data subjects have the right to have their personal data directly transmitted from one controller to another. This right is guaranteed as long as it does not affect the rights and freedoms of others.
- **Object.** Data subjects have the right to object to the processing of data relating to them at any time on compelling legitimate grounds relating to their particular situation. This right also exists on request in the case of processing for the purposes of direct marketing.

  The controller must notify the data subject of their right to object clearly and separately from any other information, at the time of the first communication with the data subject.

14. Do data subjects have a right to request the deletion of their data?

The GDPR provides that data subjects have the right to obtain from the controller the erasure of personal data concerning them without undue delay. The controller must erase such data without undue delay if one of the following grounds applies:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- The data subject withdraws the consent on which the processing was based and there is no other legal ground for the processing.
- The data subject objects to the processing (*see Question 13*).
- The personal data has been unlawfully processed.
- The personal data must be erased to comply with a legal obligation in EU or member state law to which the controller is subject.
- The personal data has been collected in relation to the offer of information society services (for children of up to 16 years of age).

If the controller has made the personal data public and must erase the personal data, it must inform any other controller who processes the data that the data subject has requested its erasure.

These provisions do not apply if the processing is necessary for.

- Exercising the right of freedom of expression and information.
- Compliance with a legal obligation that requires processing by a EU or member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Reasons of public interest in the area of public health.
- Archiving purposes in the public interest, or scientific or historical research or statistical purposes.
- The establishment, exercise or defence of legal claims.

Security requirements

15. What security requirements are imposed in relation to personal data?

Data controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk represented by the personal data processing. Those measures must take into account the:

- State of the art.
- Costs of implementation.
- Nature, scope, context and purposes of the processing.
- Varying risks for the rights and freedoms of natural persons.

These measures can include, among other things:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of an incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisation measures for ensuring the security of the processing.

In assessing the appropriate level of security, data processors must take into account the risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

Compliance with these requirements can be demonstrated by adhering to an approved code of conduct or an approved certification mechanism.

Data controllers and processors must take reasonable steps to ensure that any natural person acting on their behalf with access to personal data does not process the data except on instructions given by the controller, unless required to do so by law.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

Under the GDPR, if a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject without undue delay.

The controller must also notify the personal data breach to the National Data Protection Commission (CNPD) without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the CNPD is not made within 72 hours, the controller must justify the reasons for the delay.

Both the data subject and the CNPD must be provided with the following information:

- The name and contact details of the DPO.
- The likely consequences of the personal data breach.
- The measures taken or proposed by the controller to address the personal data breach.

In addition, the notification to the CNPD must describe the nature of the personal data breach including, if possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

However, the data subject need not be informed of the breach if any of the following conditions are met:

- The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach.
- The controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is not likely to materialise.
- It would involve disproportionate effort. The notification is then replaced by a public communication or similar measure.

The Law dated 30 May 2005, as amended, concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector (Electronic Communications Protection Law) requires a provider of publicly available electronic communications services to notify a personal data breach to the CNPD without undue delay. The notification must describe the consequences of the personal data breach, and the measures proposed to be taken or already taken by the provider.

Processing by third parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

A controller that has processing carried out on its behalf must choose a processor that provides sufficient guarantees in respect of the technical security and organisational measures governing the processing, and must ensure compliance with those measures.

Data processing by a third party must be governed by a contract or legal act binding the processor to the controller and providing in particular that:

- Data processors only process data on instructions from the data controller.
- Data processors subject their own subcontractors to the same obligations.

Electronic communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Electronic Communications Protection Law provides that storage of information or access to information already stored in the terminal equipment of a subscriber or user, is only permitted if the subscriber or user is provided with clear and comprehensive information about the purposes of the data processing.

The Electronic Communications Protection Law also expressly specifies that:

- The methods of providing information and of offering the right to refuse must be as user-friendly as possible.
- Where it is technically possible and effective, the user's consent to processing can be expressed by using the appropriate settings of a browser or other application.

This does not prevent technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as is strictly necessary to provide an information service explicitly requested by the subscriber or user.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The sending of unsolicited electronic commercial communications is regulated by the:

- Law of 14 August 2000 on electronic commerce, applicable to the sending of communications by a provider of information society services (Law on E-commerce).
- Electronic Communications Protection Law.

Under the Law on E-commerce, a provider of commercial goods or services must obtain potential customers' prior consent before sending unsolicited commercial communications.

The Electronic Communications Protection Law only allows the transmission of unsolicited communications for the purposes of direct marketing with the prior consent of the subscriber or user concerned.

If providers obtain the electronic addresses of their customers through the sale of a product or service, they can use those email addresses for commercial or marketing purposes and send commercial communications to those customers by electronic means. However, customers must have had a clear and distinct opportunity to oppose, free of charge, the use of their electronic address. Customers must be able to oppose such use at the time of the collection of their email address and in any new commercial communications.

Any unsolicited electronic commercial communications must comply with the following conditions:

- Providers must regularly consult and respect the "opt-out" registers designated by Grand-Ducal regulations, where natural persons who do not wish to receive this type of communication can register. (The registration of natural persons on one or more opt-out registers is free of charge.)
- The commercial communication must be identified as such, in a clear and unambiguous manner, on receipt by the addressee.
- The provider must be clearly identified.
- Raffles and promotional games must be clearly recognisable as such, and their conditions of participation must be easily accessible and presented in a precise and unambiguous manner.

The Electronic Communications Protection Law prohibits the sending of electronic mail for the purpose of direct marketing:

- While disguising, concealing or misrepresenting the identity of the sender.
- Without a valid address to which the recipient can send a request that such communications cease.

International transfer of data

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

Data can only be transferred to companies located in a country that provides an adequate level of protection. A transfer of personal data to a third country or an international organisation can take place if the EU Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the

international organisation in question, ensures an adequate level of protection. Such a transfer does not require any specific authorisation. The following countries have been confirmed by the European Commission as having an adequate level of protection:

- Andorra.
- Argentina.
- Canada.
- Faroe Islands.
- Guernsey.
- Israel.
- Isle of Man.
- Jersey.
- New Zealand.
- Switzerland.
- Uruguay.
- The US.

In the absence of a decision from the European Commission, a controller or processor can transfer personal data to a third country or an international organisation only if the controller or processor has provided the appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Without requiring any specific authorisation from a supervisory authority (the CNPD), the appropriate safeguards can be provided for by:

- A legally binding and enforceable instrument between public authorities or bodies.
- Binding corporate rules.
- Standard data protection clauses adopted by the European Commission.
- Standard data protection clauses adopted by a supervisory authority and approved by the European Commission.
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including in relation to data subjects' rights.
- An approved certification mechanism, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including in relation to data subjects' rights.

Subject to authorisation from the competent supervisory authority, the appropriate safeguards can also be provided for, in particular, by either:

- Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

- Provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights.

In the absence of an adequacy decision or appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organisation can take place only on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register that:
    - is intended to provide information to the public EU or member state law; and
    - is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest,

    This applies only to the extent that the conditions laid down by EU or member state law for consultation are fulfilled in the particular case.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

The GDPR does not provide any requirement to store any type of personal data inside Luxembourg.

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements are in use. The CNPD verifies whether such agreements provide sufficient guarantees for the data subjects. The CNPD recommends the use of standard contractual clauses approved by the European Commission.

The CNPD also approves binding corporate rules (BCRs) that regulate the transfer agreements inside a group of undertakings. BCRs must specify the:

- Structure and contact of the group of undertakings.
- Data transfers to be made.
- Legally binding nature of the BCR.
- Application of the GDPR principles.
- Rights of data subjects.
- Acceptance of liability by the controller for any breaches.
- Provision of information on the BCR to the data subjects.
- Tasks of the DPO (if applicable).
- Complaint procedures.
- Mechanisms for reporting and recording changes to the BCR.
- Co-operation mechanisms with the supervisory authority to ensure compliance.
- Mechanisms for reporting any legal requirements to the competent supervisory authority.
- Appropriate data protection training for personnel with access to personal data.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer must be based either on the consent of the data subject or on a data transfer agreement.

24. Does the relevant national regulator need to approve the data transfer agreement?

The CNPD does not need to approve the data transfer agreement (*see Question 20*).

Enforcement and sanctions

25. What are the enforcement powers of the national regulator?

The CNPD has investigative powers to:

- Order the controller and the processor, and, where applicable, the controller's or the processor's representative, to provide any information the CNPD requires for the performance of its tasks.
- Carry out investigations in the form of data protection audits.
- Review issued certifications.
- Notify the controller or the processor of an alleged infringement of the GDPR provisions.
- Obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks.
- Obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with EU or member state procedural law.

The CNPD has corrective powers to:

- Issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR.
- Issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR.
- Order the controller or the processor to comply with the data subject's requests to exercise their rights under the GDPR.
- 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.
- Order the controller to communicate a personal data breach to the data subject.
- Impose a temporary or definitive limitation including a ban on processing.
- Order the rectification or erasure of personal data or restriction of processing.
- Withdraw a certification or order the certification body to withdraw an issued certification, or order the certification body not to issue certification if the requirements for the certification are not or are no longer met.

- Impose an administrative fine, in addition to, or instead of other measures, depending on the circumstances of each individual case.
- Order the suspension of data flows to a recipient in a third country or to an international organisation.

The CNPD has authorisation and advisory powers to:

- Advise the controller in accordance with the prior consultation procedure.
- Issue, on its own initiative or on 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.
- Authorise processing by a controller for the performance of a task carried out by the controller in the public interest, if the law of the member state requires prior authorisation.
- Issue an opinion and approve draft codes of conduct.
- Accredit certification bodies.
- Issue certifications and approve certification criteria.
- Adopt standard data protection clauses.
- Authorise contractual clauses.
- Authorise administrative arrangements.
- Approve binding corporate rules.

26. What are the sanctions and remedies for non-compliance with data protection laws?

Among the corrective measures (*see Question 25*), the GDPR provides for administrative fines for infringements of up to:

- EUR10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher) for an infringement relating to the following provisions:
    - the conditions applicable to a child's consent in relation to information society services;
    - processing that does not require identification;
    - data protection, by design and by default;
    - the tasks of the DPO and certification;
    - the obligations of the certification body; or
    - the obligations of the monitoring body.

- EUR20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher) in the event of an infringement relating to the following provisions:
  - the basic principles for processing (conditions for consent, and so on);
  - data subjects' rights;
  - transfers of personal data to a recipient in a third country or an international organisation;
  - any obligations under member state law regarding specific processing regulations; or
  - non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

Regulator details

National Commission for Data Protection (*Commission Nationale pour la Protection des Données*) (CNPD)
W *www.cnpd.lu*

Main areas of responsibility. The CNPD is responsible for ensuring that data is processed in accordance with the provisions of the GDPR and the Electronic Communications Protection Law.

The CNPD also:

- Supervises and checks the legality of collecting and using data to be processed, and informs the parties carrying out the processing of their obligations.
- Ensures personal freedoms and fundamental rights, particularly as regards to privacy, and informs the public of the personal rights involved.
- Receives and examines complaints and requests for checks on the legality of processing.
- Advises the government.

Online resources

National Commission for Data Protection (*Commission Nationale pour la Protection des Données*) (CNPD)
W *www.cnpd.lu*

Description. The official website of the National Data Protection Commission.

General Data Protection Regulation
W *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en*

Description. English version of the General Data Protection Regulation.

Contributor profile

Anne Morel, Partner and Head of the Employment, Compensations & Benefits practice

Bonn Steichen & Partners

T +352 26 0251
F +352 26 025 999
E *amorel@bsp.lu*
W *www.bsp.lu*

Professional qualifications. Admitted to the Luxembourg Bar, 1994; Université Nancy II, France, *DESS en Droit des Affaires et Fiscalité - Diplôme de Juriste Conseil d'Entreprise* (Post-Graduate Degree in Business Law and Tax Law),1993; Université Nancy II, France/University of Saarbrücken, Germany, *Maîtrise en Droit des Affaires* (Masters in Business Law), 1992

Areas of practice. Employment, compensations and benefits; general commercial; data protection.

Recent transactions

- Launch of a new product by a multinational company based in the US enabling its customers to set up a WIFI network that is hosted and managed via a local cloud.
- Setting up of a shared service centre in Malaysia for a client, with the aim to providing finance related services to regional subsidiaries.
- Implementation of a centre of information for our client including the personal data regarding the employees.
- Legal assistance in respect of the implementation of a mobile data communication services in a device incorporated into cars.
- Legal assistance in relation to the initiation of a cloud compliance project to identify and review all existing cloud services used by a client to ensure compliance with mandatory legislation.
- Legal assistance in relation to the implementation of a data centre in Luxembourg, and assistance in the filing of notifications with local authorities.
- Reviewed an EC Model Clause data transfer agreement and flagging any potential issues with any of the proposed data transfers. Provided an overview of the filings/authorisations/process needed

to enable the client to transfer the relevant personal data to the US based on the model clause agreement. Completed filings and authorisations necessary to enable the transfers.

Languages. English, French, German

Professional associations/memberships. Employment Law Specialists Association, Luxembourg (ELSA); European Employment Lawyers Association (EELA); International Bar Association (IBA); Industrial Relations & Social Affairs Committee of The Luxembourg Bankers' Association (ABBL); Insol Europe (INSOL); Member of Bar Council, 2014-2015 & 2015-2016.

Publications

- *Maximale Prävention und vorherige Sperrung, Journal, July 2016.*
- *La cour d'appel rappelle les règles applicables aux centres d'affaires, Entreprises Magazine, March/April 2016.*
- *Workforce Restructuring in Europe, Bloomsbury Professional, 2015.*
- *The Anti-Bribery and Anti-Corruption Review Luxembourg, The Law Reviews Ltd, editions 2015, 2016, 2017.*
- *The Executive Remuneration Review Luxembourg, The Law Reviews, editions 2015, 2016, 2017.*
- *The Intellectual Property Review Luxembourg, The Law Reviews, editions 2015, 2016, 2017.*

END OF DOCUMENT

