GUIDANCE NOTE

Luxembourg - Data Transfers

Vincent Wellens
NAUTADUTILH

Sigrid Heirbrant
NAUTADUTILH

November 4, 2024

November 2024

1. Governing Texts

1.1. Legislation

In Luxembourg, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) has been implemented into domestic law by the Act of 1 August 2018 on the Organisation of the National Commission for Data Protection and Implementing the GDPR (the Data Protection Act).

The Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680) (the Law Enforcement Directive) has been transposed into domestic law by the Act of 1 August 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 Data Protection in Criminal Matters Act).

On the one hand, the Data Protection Act contains provisions relating to the establishment, powers, and operation of the National Commission for Data

Protection (CNPD), i.e., the Luxembourg data protection authority. On the other hand, it includes specific provisions completing the GDPR at a national level, such as provisions relating to the processing of personal data for the sole purpose of journalism or academic, artistic, or literary expression, for scientific, historical research, or statistical purposes, or for the purposes of surveillance in the employment context.
Both acts entered into force on August 20, 2018.

At the outset, it can already be noted that both acts do not contain many derogations on the provisions of Chapter V of the GDPR when it comes to international data transfers. Furthermore, the two other key domestic legislative acts within the context of the exchange of information and personal data for the purpose of cross-border cooperation in criminal matters are the following:

- Act of 29 March 2013 on the Organisation of the Criminal Record and the Exchange of Information from the Criminal Record among EU Member States (as amended) (only available in French here); and
- Act of 22 December 2006 on the Ratification of the Treaty between Belgium, Germany, Spain, the Netherlands, France, Austria, and Luxembourg concerning Cross-border Cooperation, particularly in terms of Combating Terrorism, Cross-border Crime, and Illegal Migration, as well as their Common Declaration (only available in French here).

The CNPD has issued guidance on international data transfers, namely, General Data Protection Regulation – International Data Transfers (the Guidance), which deals with:

- transfers within the European Economic Area (EEA);
- transfers outside the EEA with adequate protection;
- transfers outside the EEA without adequate protection; and
- international cooperation in the field of Police and Justice.

In addition, the CNPD issued a brief statement following the invalidation of the Privacy Shield in the Court of Justice of the European Union's (CJEU) judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) (Schrems II) (see section on usage of data transfer agreements/standard contractual clauses below). Another brief statement was issued following the adoption of the EU-US Data Protection Framework.

None of Your Business (NOYB), the non-profit organization founded by Max Schrems, has filed 101 complaints against EU companies for transferring data to Facebook and Google post-Schrems II, three of which against Luxembourg organizations before the CNPD. These cases are pending. According to NOYB, the CNPD dismissed the claims. To the contributors' knowledge, the decisions have not been published by the CNPD.

Further to Brexit, the CNPD issued a thematic dossier Guidance on Brexit – The Consequences of Brexit for International Data Transfers (only available in French here) to offer guidance to companies, public bodies, and associations in Luxembourg that may transfer personal data to the UK and intend to pursue such transfers in 2021 and beyond. Since the Commission Implementing Decision Pursuant to Directive (EU) 2016/680 on the Adequate Protection of Personal Data by the United Kingdom adopted by the European Commission (European Commission) on June 28, 2021, personal data transfers to the UK can be made as if they were transfers within the EEA.

1.2. Case law

In July 2019, in Decision No. 43/2019 (only available in French here), the CNPD authorized the Financial Sector Supervisory Commission (CSSF) to transfer data to financial market authorities in third countries for which the European Commission had not rendered adequacy decisions.

The CSSF is a party to the International Organization of Securities Commissions (IOSCO) Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU) pertaining to the consultation, cooperation, and exchange of information among the international community of securities regulators. However, this MMoU does not address the issue of the protection of personal data. Hence, in order to comply with the GDPR, the parties to the MMoU have elaborated an administrative arrangement in accordance with Article 46(3)(b) of the GDPR covering personal data transfers outside the EEA. In the above decision, the CNPD approved this administrative arrangement, and authorized, upon certain conditions, the transfer of personal data to financial market authorities in third countries.

In Decision No. 67/20 of 6 May 2020 (only available in French here) in the context of summary proceedings, the Court of Appeal prohibited the transfer of personal data relating to certain bank accounts by a Swiss bank to the U.S. Department of Justice or any other American authority. The bank in question was subject to

criminal proceedings in the US and sought reduced sentences by means of such disclosure. The data subject concerned refused to consent to such transfer. The fact that the data was pseudonymized was deemed irrelevant by the Court. The bank was not able to produce sufficient evidence that it could rely on one of the grounds in Article 49 of the GDPR to justify the transfer, nor any other ground laid down in Chapter V of the GDPR. In Decision No. 141/23 of 6 December 2023 (only available in French here), in the context of the proceedings on the merits, the Court of Appeal confirmed the measures taken in the summary proceedings. In both proceedings, it is relevant to note that in the first instance, the District Court adopted an approach contrary to the Court of Appeal through a narrower understanding of the concept of personal excluding beneficial ownership therefrom, an exclusion which the Court of Appeal overturned.
The CNPD decisions published in 2021 and 2022 related, for the largest part, to the thematic investigation campaigns on video surveillance practices, the role of the data protection officer (DPO), and geolocation of employees.

Just as in 2021 and 2022, in 2023, the decisions related for the most part to (non-international) transfers of data to a third party, video surveillance and geolocation as well as to transparency in the e-commerce sector.

In decision No. 13/23 of 21 September 2023, (only available in French here), the CNPD criticized an organization for having misinformed data subjects regarding the processing of their personal data as part of an international transfer of data between the EU and the US. In this instance, the data controller based the international transfer on the Privacy Shield decision which was no longer valid at the time of the transfer.

However, so far, the CNPD has not published a landmark decision regarding international data transfers.

2. Definitions

The Data Protection Act does not contain definitions added to the GDPR. Consequently, GDPR definitions are thus fully applicable, including:

Personal data: any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of such personal data.

Controller: the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. EU or Member State law may detail the controller or the specific criteria for their nomination in cases where the purposes and means of processing are determined by the respective laws.

Processor: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Group of undertakings: a controlling undertaking and its controlled undertakings.

Binding corporate rules (BCRs): personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Cross-border processing: either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the EU but which

substantially affects or is likely to substantially affect data subjects in more than one Member State.

International organization: an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

The Data Protection in Criminal Matters Act adopts the definitions of the Law Enforcement Directive.

3. Scope of Application

The Data Protection Act extends the scope of application of the GDPR.

Pursuant to Article 1 of the Data Protection Act, any processing of personal data that is not covered by the GDPR or the Data Protection in Criminal Matters Act, is covered by the provisions of Chapter I, Article 4, and the provisions of Chapter II to VI, VIII and IX, and Chapter VII, Section 1 of the GDPR and the Data Protection Act, subject to existing legal texts containing other specific provisions relating to personal data protection.

From a territorial point of view, Title II of the Data Protection Act containing specific provisions relating to the processing for journalistic purposes, research purposes, and in the employment context, applies to controllers and processors established on Luxembourg territory.

The Data Protection in Criminal Matters Act applies to any competent public authority processing personal data for the purposes of the prevention and detection of criminal offenses, criminal investigations and prosecutions, and the execution of criminal sanctions. It also applies to the processing of personal data by the Luxembourg Police, State Intelligence Service, National Security Authority, Luxembourg Army, Financial Intelligence Unit, and the Luxembourg authorities in relation to their activities within the context of the EU's Common Foreign and Security Policy (Title V, Chapter II of the Treaty on European Union). Lastly, the Data Protection in Criminal Matters Act applies to the (fully or partially) automated processing of personal data and the non-automated processing of personal data contained or to be included in a filing system.

4. Restrictions on the Transfer of Data

4.1. Within jurisdiction/region

Provided that the general principles of the GDPR, the Data Protection Act, and the Data Protection in Criminal Matters Act are respected, there are currently no specific restrictions imposed by Luxembourg law on the transfer of data within Luxembourg.

4.2. Outside of jurisdiction/region

Since neither the Data Protection Act nor the Data Protection in Criminal Matters Act contain specific restrictions on data transfers within the EEA, personal data may be freely transferred to countries within the EEA. The free flow of personal data within the EEA is one of the key principles of the GDPR.

For transfers outside the EEA, Chapter V of the GDPR applies. Only Article 62 of the Data Protection Act explicitly excludes the application of Chapter V of the GDPR relating to transfers to third countries if personal data is transferred to third countries for the sole purpose of journalism, or academic, artistic, or literary expression.

Articles 34-38 of the Data Protection in Criminal Matters Act provide for specific principles and conditions for international transfers of personal data by competent authorities for the purposes of the prevention, detection, investigation, and prosecution of criminal offenses or the execution of criminal penalties, including the prevention of and protection against dangers for public security.

In general, the CNPD recommends in the Guidance mentioned in the section on the law above, a layered approach to transfers to countries outside the EEA without an adequate level of protection, consisting of:

- verifying if the third country provides an adequate level of protection, ensuring that the exported data will be safeguarded in that country;
- if there is no adequacy decision, endeavoring to apply appropriate safeguards to the transfer, as provided for by Article 46 of the GDPR; and

- only in the absence of such guarantees, data exporters should use the derogations provided for in Article 49 of the GDPR.

In addition, in Luxembourg, the consequences of the Schrems II judgment must be taken into account in the context of personal data transfers to a third country for which no adequacy decision has been adopted.

In light of the Schrems II judgment, the Commission and United States announced, on March 25, 2022, that they had confirmed an agreement in principle for a new Transatlantic Data Privacy Framework to facilitate data transfers between the EU and US.

The White House announced, on October 7, 2022, that President, Joseph Biden, had signed, on the same date, an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (the Executive Order), which outlined the steps that the US would take to implement its commitments under the European Union - US Data Privacy Framework (EU-US DPF). In light of this, the Attorney General, Merrick Garland, signed, on the same date, the regulation establishing the Data Protection Review Court (the Regulations).

In response to the above, on July 10, 2023, the European Commission voted to adopt its adequacy decision for the EU-US DPF, concluding that the US provides a level of protection essentially equivalent to that of the EU for personal data transferred under the EU-US DPF from a controller or a processor in the EU to self-certified organizations in the US. The adequacy decision has the effect that personal data transfers from controllers and processors in the EU to self-certified organizations in the US may take place without the need to obtain any further authorization.

5. Data Localization

Neither the Data Protection Act nor the Data Protection in Criminal Matters Act contain any general data localisation or residency requirements. Nevertheless, the CSSF has issued sector-specific regulations that may affect data residency. For example, the CSSF Circular 22/806 – Outsourcing Arrangements (Circular

22/806), requires resiliency of cloud computing services, and therefore the localization of at least one data center in the EEA.

6. Sector-Specific Restrictions

Health data

Neither the Data Protection Act nor the Data Protection in Criminal Matters Act impose specific restrictions or conditions for the international transfer of health data. However, by virtue of the Law of 17 December 2010 reforming the Healthcare System (only available in French here), an electronic national platform, namely, eSanté, has been set up for the exchange of health data among different actors in the healthcare sector in Luxembourg. Furthermore, the Grand-Ducal Regulation of 6 December 2019 specifying the Modalities and Conditions for the Establishment of the Shared Record of Care (only available in French here), which came into effect on January 1, 2020, contains provisions regulating the transfer of health data to the relevant EU/EEA authorities in the context of shared records of care.

Lastly, as from 2020, Luxembourg offers electronic cross-border health services (only available in French here) that will allow the exchange of patient summaries among healthcare professionals in the EU, on the basis of the patient's explicit consent.

Financial data

Neither the Data Protection Act nor the Data Protection in Criminal Matters Act impose specific restrictions or conditions for the international transfer of financial data. However, the CNPD Decision No. 43/2019 (see section on case law above) imposes certain conditions for the transfer of data by the CSSF towards financial market authorities in third countries for which the European Commission has not rendered adequacy decisions. Some indirect restrictions further follow from financial sector regulations which contain rather strict rules on outsourcing. Outsourcing transactions often involve data flows from Luxembourg to a country abroad, and regulatory restrictions applicable to outsourcing also make the transfer of data abroad more difficult.

HR/employee data

Neither the Data Protection Act nor the Data Protection in Criminal Matters Act impose specific restrictions or conditions for the international transfer of personal data in the HR/employment context.

7. Data Transfer Solutions

7.1. Legislative exceptions to the restrictions

Article 62 of the Data Protection Act explicitly excludes the application of Chapter V of the GDPR relating to transfers to third countries if personal data is transferred to third countries for the sole purpose of journalism, or academic, artistic, or literary expression.

7.2. Usage of data transfer agreements/standard contractual clauses

Chapter V of the GDPR fully applies, as well as the requirements introduced by CJEU case law, such as the Schrems II judgment (see above).

As the CSSF is party to the MMoU, it has an obligation to consult, cooperate, and exchange information with the securities regulators of third countries, parties to the MMoU. The transfer of personal data towards such authorities outside the EEA is based on an administrative arrangement within the meaning of Article 46(3)(b) of the GDPR and approved by the CNPD. To the writers' knowledge, the CNPD has yet to adopt any specific standard data protection clauses.

7.3. Usage of intragroup agreements, BCRs, CBPRs

Chapter V of the GDPR fully applies, as well as the requirements introduced by CJEU case law, such as the Schrems II judgment (see above).

The procedure for the approval of BCRs consists of multiple steps to be taken and includes the identification of a lead authority coordinating the cooperation procedure with other European data protection authorities (DPAs). In 2018, for

example, the CNPD acted as lead authority and approved the BCRs of the PayPal group. Following the analysis made by the CNPD, all EU DPAs approved the decision of the CNPD, and agreed to provide the necessary permit or authorization at a national level for transfers of personal data in the context of those BCRs.

7.4. Usage of whitelists and international treaties

Chapter V of the GDPR fully applies.

In addition, Luxembourg has signed up to the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities (the Declaration) which clarifies how national security and law enforcement agencies can access personal data under existing legal frameworks.

Specifically, the Declaration's principles set out:

- how legal frameworks regulate government access;
- the legal standards that should be applied when access is sought;
- how access is approved and how the resulting data is handled; and
- efforts by countries to provide transparency to the public.

Furthermore, the Declaration also outlines requirements for oversight and redress, providing that there should be mechanisms for effective and impartial oversight to ensure that government access complies with the legal framework, and that the legal framework should provide individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework.

7.5. Other solutions

Chapter V of the GDPR fully applies.

7.6. Notification/approval requirements for the above

Not applicable.

8. Sanctions

Pursuant to Article 48 of the Data Protection Act, the CNPD may impose administrative fines as set out in Article 83 of the GDPR, except against the Luxembourg State and municipalities, for infringements of the provisions relating to the international transfers of personal data.

Pursuant to Article 47(1) of the Data Protection in Criminal Matters Act, violations of the data transfer rules in Articles 34-38 of the Data Protection in Criminal Matters Act may be subject to an administrative fine between €500 and €250,000.

Violations of CSSF Circulars, such as Circular 22/806 as amended, may incur administrative fines, as well as other sanctions provided for in Law of 5 April 1993 on the Financial Sector, as amended.

Topics: Data Transfers

Jurisdictions: Luxembourg