Newsletter

EHLO, our ICT, IP, media and data protection news - (M)ovember 2020

CJEU clarifies legality of surveillance legislation for national security

What happened?

Recently, the Court of Justice of the European Union (" **CJEU**") ruled on case C-623/17[1] and the joined cases C-511/18, C-512/18[2] and C-520/18[3] (the "**Joined Cases**") on the lawfulness of national security laws of the United Kingdom, France and Belgium, respectively, which each require electronic communications services providers (the "**Service Providers**") to retain and disclose traffic and location data of their respective users to national authorities for the purpose of combating crime or safeguarding national security. The CJEU provided some important clarifications on the circumstances in which traffic and location data can be collected and retained.

What clarification did the CJEU provide?

National security is within the competence of each EU Member State. However, the CJEU clarified that national legislation requiring Service Providers to retain and disclose users' locations and traffic data to public authority falls within the scope of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (the **"ePrivacy Directive"**). Consequently, those legislative measures have to comply with the general principles of European Law and the Charter of Fundamental Rights of the European Union (the "**Charter**").

It follows that Member States cannot restrict the scope of the ePrivacy Directive unless such restrictions comply with the general principles of EU law, are proportionate and preserve the fundamental rights guaranteed under the Charter.

Derogation regarding targeted surveillance

However, the Court did formulate certain derogations regarding the scope of the ePrivacy Directive. More precisely, the Court specified that the ePrivacy Directive does not prevent:

- the recourse of a Member State to an order requiring Service Providers to retain traffic and location data generally and indiscriminately, only if that Member State faces a serious threat to national security that proves to be genuine and present or

foreseeable; and

- the recourse of Member States to the targeted retention of traffic and location data (1) limited in time to what is strictly necessary and (2) limited on the basis of objective and non-discriminatory factors, according to the categories of persons concerned, or by using a geographical criterion.

The CJEU framed how targeted surveillance can comply with the ePrivacy Directive and existing EU Laws.

Derogations regarding real-time collection

EU Member States may adopt legislative measures requiring Service Providers to collect traffic and location data in real time provided that the collection is based

- on a genuine and present or foreseeable serious threat to national security; or
- concerns persons suspected of being involved in terrorist activities.

By this recent ruling, the Court clarified a framework under which Member States can adopt laws under which Service Providers are required to retain and disclose traffic and location data to supervisory authorities.

This may also interest you :

- 5G: Opportunities and Legal Challenges
- 5G: Opportunities and Legal Challenges - Part 2. Deployment of 5G in Luxembourg
- Draft Law implementing the European Electronic Communications Code in Luxembourg

1 Privacy International v. United Kingdom.

2 La Quadrature du Net & Others v. France.

3 Ordre des barreaux francophones and germanophones & Other v. Belgium.

EDPB Guidelines 07/2020: update on the concepts of controller and processor

What happened?

On 2 September 2020, the European Data Protection Board (" **EDPB**") adopted its draft Guidelines 07/2020 on the concepts of controller and processor in the GDPR ("**Guidelines**"). The Guidelines, once adopted, will replace the Opinion 1/2010 adopted by the Article 29 Data Protection Working Party[1] with the objective to provide updated guidance on the concepts of controller and processor and further clarify their different roles and responsibilities in the light of the General Data Protection Regulation ("**GDPR**")[2].

Reminder: how to determine the roles of controller and processor?

The roles of controller and processor are crucial since they determine who shall be responsible for complying with certain specific rules under the GDPR. However, those concepts are not always easy to ascertain in practice. The Guidelines intend to keep a consistent approach throughout the European Union on the circumstances to consider when identifying controllers and processors.

As a reminder, the controller is the person who determines the purposes and/or (essential) means of an identified personal data processing whereas the processor processes the personal data on behalf of the controller and under its instructions. Such roles are determined on a case-by-case basis against the factual background at hand (e.g. contractual relationships, competence conferred by law, traditional role and professional expertise).

Accordingly, the identification of an entity as a controller or a processor does not depend on that entity's nature but results from its concrete activities in relation to a specific personal data processing in a specific context. Therefore, the same entity may (and most of the time will) act at the same time as controller for specific processing and as processor for others within a given or related context. It also means that the contractual terms between the parties involved are not decisive in all circumstances since the assessment of the roles of the parties is a matter of fact. Similarly, not every service provider processing personal data in the course of delivering its services is a processor, even if that is explicitly stated in a contract between the service provider and its client.

What's new in the Guidelines?

Without being exhaustive here, the Guidelines specifically address and clarify the level of details to be provided in the processing agreement to be entered into between controllers and processors under Article 28.3 GDPR. In particular:

- it should not merely restate the provisions of the GDPR, but provide for specific and concrete information as to how the GDPR requirements will be met;
- it should include a list of authorised sub-processors, if any, together with the details of their processing activities, locations and implemented safeguards;
- any intended modification of the processing agreement must be expressly notified to and approved by the controller; the mere publication of such modifications on the processor's website does not comply with Article 28 of the GDPR;
- it is not required that the processing agreement between the processor and any subsequent processor includes provisions identical to those between the controller and the processor but similar obligations may be sufficient as appropriate according to the context; in the event that certain obligations cannot apply to the subsequent processor, such obligations should not be included by default in the contract.

The EDPB states again that processing agreements entered into between controllers and processors before 25 May 2018 must already have been updated to comply with the GDPR. The imbalance in contractual power between a controller and a processor cannot be a justification for the controller to accept contractual terms that are not GDPR-compliant.

What's next?

This version of the Guidelines was subject to public consultations until 19 October 2020. After analysing the contributions received, the EBPD will adopt a final version of the Guidelines. Stay tuned!

This may also interest you :

- EDPB's FAQ about the invalidation of the Privacy Shield
- EDPB's updated Guidelines on consent under GDPR: cookies and scrolling
- EDPB Recommendations 01/2020 and 02/2020 on transfers of personal data after Schrems II

1 Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) adopted on 16 February 2010. The Article 29 Data Protection Working Party was succeeded by the EDPB on 25 May 2018.

2 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

EDPS publishes its strategy for Union institutions' compliance with "Schrems II" ruling

What is the context of this Strategy?

On July 16 July 2020, the CJEU issued its ruling related to the "Schrems II" case (C-311/18) (the "**Schrems II Ruling**") invalidating the EU-US Privacy Shield Framework but also affecting the manner in which EU Standard Contractual Clauses may have to be implemented in the future as a safeguard for extra-EEA data transfers[1].

In this context, the EDPS[2] published a strategy on 29 October 2020 (the " **Strategy**") in order to ensure that the bodies, offices and agencies of European Union Institutions ("**EUIs**") comply with the requirements deriving from the Schrems II Ruling. The Strategy's main goal is therefore to ensure that ongoing and future international transfers as implemented by such EUIs comply with applicable data protection regulations[3] as read in light of the Schrems II Ruling.

What is the content of the Strategy?

The Strategy relies on a twofold approach, based on short- and mid-term actions as further detailed below.

As a short-term compliance action:

The EDPS issued an order to EUIs to complete a mapping exercise for identification of ongoing contracts, procedures and any other types of cooperation involving transfers of data. EUIs are then expected to report to the EDPB by 15 November 2020 at the latest on specific risks and gaps they identified during this mapping exercise, in particular by taking into account certain types of transfers which may present a high risk for the rights and freedoms of individuals such as transfers to U.S. entities subject to Section 702 FISA[4] or E.O.[5] 12333, and involving either large-scale processing operations, complex processing operations or the processing of sensitive personal data.

As a medium-term compliance action:

The EDPS will provide guidance and pursue enforcement actions for transfers towards the U.S. or other third countries on a case-by-case basis. In this context, EUIs will be asked to carry out Transfer Impact Assessments (**"TIAs"**) to identify whether a specific transfer at stake benefits from an equivalent level of protection as provided in the EU/EEA with subsequent reporting to the EDPS based on the outcome of the TIAs.

The EDPS will also contemplate the possibility to perform joint assessments of levels of protection of personal data with other relevant authorities and stakeholders while also cooperating with the EDPB[6] on the development of further guidance and recommendations.

This may also interest you :

- CJEU invalidates the Privacy Shield: implications for EU-US personal data transfers
- EDPB's FAQ about the invalidation of the Privacy Shield
- EDPB Recommendations 01/2020 and 02/2020 on transfers of personal data after Schrems II

1 Please read our full comment of the Schrems II case here.

2 European Data Protection Supervisor: the body in charge of ensuring the protection of personal data and privacy throughout all EU institutions.

3 In particular with Chapter V of the (EU) Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, known as the EUDPR – the equivalent of the General Data Protection Regulation for EUIs.

4 Foreign Intelligence Surveillance Act.

5 Executive Order.

6 European Data Protection Board.

EDPB Recommendations 01/2020 and 02/2020 on transfers of personal data after Schrems II

For an outlook of the latest development as at July 2023 in relation to transfers to the US, please read our article about the New EU adequacy decision allowing personal data transfers to US self-certified entities!

What happened?

On 10 November 2020, the European Data Protection Board (**"EDPB"**) adopted two sets of recommendations on the transfer of personal data from the European Union ("**EU**") to third countries further to the Court of Justice of the European Union ("**CJEU**") ruling in the

Schrems II case[1]:

- Recommendations 01/2020 on measures that supplement data transfer tools to ensure compliance with the EU level of protection of personal data (**"Recommendations on Supplementary Measures"**), open for public consultation; and

- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (**"EU Essential Guarantees")**.

Significance of these recommendations

These two sets of recommendations were highly anticipated by businesses and organisations with regard to the CJEU's (i) invalidation of the EU-US Privacy Shield and (ii) call for compliance with the requirements to be me for standard contractual clauses ("**SCCs**") to be valid in practice under the EU General Data Protection Regulation ("**GDPR**").[2] Although the ruling, aside from the EU-US Privacy Shield, only concerns the standard contractual clauses, the principles set out by the ruling equally apply to other transfer mechanisms, such as the binding corporate rules.

In a nutshell, the Recommendations on Supplementary Measures provide for a road map of good practices for data exporters while the EU Essential Guarantees outline certain features that need to be evaluated to assess whether the legislation of the third countries governing access to personal data by public authorities is to be regarded as a justifiable interference or not.

What are the main practical takeaways?

In its Recommendations on Supplementary Measures, the EDPB suggests following a methodology oriented around the six following steps.

- **Step 1: Know your transfers.** Data exporters should record and map all international personal data transfers and verify whether they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are operated. Organisations should aim to be fully aware of their data transfers (including onward transfers) despite the existence of numerous processors and sub-processors.

- **Step 2: Identify the transfer tools relied upon.** Organisations should identify the appropriate mechanism for the data transfer (e.g. adequacy decision, SCCs, derogation for specific situations of Article 49(1) GDPR, etc.). The EDPB notes that no further steps are required for transfers relying on an adequacy decision, provided that the data importer has implemented measures to comply with the obligations of

the GDPR as appropriate.

- **Step 3: Assess whether the transfer tool you relied upon is effective in light of all the circumstances of the transfer.** Organisations are responsible for assessing and analysing whether the laws and practices of the third countries concerned are effective enough to meet the appropriate safeguards set by the GDPR. This assessment shall include the circumstances as well as all the players participating in the transfer previously mapped in Step 1.

  Special attention should be given to the EU Essential Guarantees. According to these, organisations must:

  - Assess whether the processing is based on clear, precise and accessible rules; and
  - Evaluate the third countries' legislation providing for the disclosure of personal data to public authorities or grant public authorities powers to access personal data. The EDPB highlights that those laws must be publicly available and limited to what is regarded as justifiable interference and therefore not jeopardise the commitment taken in the appropriate safeguard concerned

- **Step 4: Adopt supplementary measures.** If the appropriate safeguard adopted for the data transfer is not effective according to the assessment in Step 3, organisations (in cooperation with data importers) will have to adopt supplementary measures along with that appropriate safeguard to attain an equivalent level of data protection, as is required by the GDPR.

- **Step 5: Adopt procedural steps if you have identified supplementary measures.** Organisations which have identified adequate supplementary measures will have to implement supplementary procedural steps or additional requirements before use.

- **Step 6: Re-evaluate at appropriate intervals.** Data exporters must continuously monitor significant developments that may affect the level of data protection in the third countries concerned. If a country has passed a new national security law, organisations might, for example, have to repeat Step 3.

What's next?

The recommendations are and constitute a first useful and practical response to the Schrems II ruling. Data exporters will have to make extra efforts and, on a case-by-case basis, assess their current and intended transfers of personal data. In parallel, data exporters must stay tuned as regards the adoption by the European Commission of updated SCCs as a new set of SCCs has now been published for public consultation.[3]

This may also interest you :

- CJEU invalidates the Privacy Shield: implications for EU-US personal data transfers
- EDPB's FAQ about the invalidation of the Privacy Shield
- EDPS publishes its strategy for Union institutions' compliance with "Schrems II" ruling

1 Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. For more information on the ruling in this Case, please read our previous publication.

2 Regulation (EU) 2016/679.

3 On 12 November 2020, the European Commission has published its draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries which will be open for public consultation until 10 December 2020. The draft SCCs can be consulted at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

5G: Opportunities and Legal Challenges - Part 2. Deployment of 5G in Luxembourg

This article is the second of a series of publications, which focuses on specific 5G topics.

Register here to follow our series of articles on the theme of 5G.

In our previous publication we presented an overview of the 5G technology and the related opportunities in our society. This publication focuses on the concrete deployment of 5G in Luxembourg and more particularly the allocation of a dedicated part of the electromagnetic spectrum.

5G: How does it work?

5G technology requires the use of the existing radio spectrum to transmit and receive signals through adequate infrastructure and end-users' equipment. However, the spectrum is a finite resource and its management has been entrusted to the State by the Law of 30 May 2005 on the management of radio waves (as amended). Accordingly, the use of radio waves whether for broadcasting or receiving signals is subject to licence in accordance with a frequency plan and a frequency register maintained by the *Institut*

Luxembourgeois de Régulation ("**ILR**").

Which frequency bands will be dedicated to 5G?

To deploy 5G, the European Union's Radio Spectrum Policy Group [1] identified three different frequency ranges: (i) the band of 700MHz (470-790 MHz), (ii) the band of 3.6 GHz (3400-3800 MHz) and (iii) the band of 26 GHz (24.25-27.5 GHz). In Luxembourg, the ILR conducted two public consultations between May and July 2019 on the allocation of parts of the 700MHz and 3.6 GHz bands. As a result, the Minister of Communications and Medias decided to allocate the bands of 703-733/758-788 MHz and the band of 3420-3750 MHz to the deployment of 5G. On 28 October 2020, the ILR launched a public consultation on the 26 GHz band (26.5 GHz to 27.5 GHz) to assess the interests and needs of potential candidates for its future use.[2] Depending on the results of that public consultation, selected parts of the 26 GHz band might also be allocated to the candidates concerned. However, it is assumed that no massive exploitation of the 26 GHz band will happen before 2025.

How are frequency bands allocated to candidates?

The frequency bands available have been allocated further to an auction organised by the ILR between 13 and 17 July 2020 with all the interested candidates.[3] As a result, all the frequencies available have been allocated to four telecom operators in July 2020 (against five candidates): Post Luxembourg, Proximus Luxembourg SA, Orange Communications Luxembourg SA and Luxembourg online SA.[4] They have been granted a licence to use the frequencies allocated to them.

What is covered/imposed by the 5G licence?

The licences are valid for an initial period of 15 years and renewable (at least once) for a further period of five years. The auction also provided for conditions and obligations to be met by the licence holders for using the allocated frequencies, in particular: (i) to comply with the agreements between the countries concerned (i.e. Luxembourg, Belgium, France, Holland and Switzerland) on cross-border coordination for the use of the radio spectrum, (ii) to comply with technical conditions as determined by the European Commission for the harmonisation of the frequency bands[5], (iii) to synchronise the networks between the different operators to avoid any interference, (iv) to protect other services using the radio spectrum (e.g. fixed-satellite service), (v) to deploy the technology and cover the territory of Luxembourg in accordance with a determined calendar and, (v) specific conditions to share the allocated frequency bands and for the transfer of related licences.

What's next?

According to the Luxembourg government calendar for the deployment of 5G, each licence holder shall equip a minimum of 10 sites with an active base station to connect all its final clients in the city of Luxembourg at the latest on 31 December 2020. On 30 June 2021, a minimum 20 sites will be required at national level, 40 sites on 31 December 2022 with a national coverage of 50% and 80 sites on 31 December 2024 with a national coverage of 90%. It is expected that all licence holders will make 5G available to their customers by the end of 2020. Meanwhile certain operators have already proposed concrete offers including the use of 5G.

This may also interest you :

- 5G: Opportunities and Legal Challenges
- Draft Law implementing the European Electronic Communications Code in Luxembourg
- Developments of the CJEU on the concept of “electronic communications service”

1 The Radio Spectrum Policy Group is an advisory group composed of representatives of the Member States and of the Commission assisting the Commission in the development of radio spectrum policy, in particular to coordinate the approach to radio spectrum management in the European Union.

2 The public consultation is open until 8 December 2020.

3 Ministerial Decision of 27 April 2020 on the procedure of competitive selection by auctioning for the allocation of the 700MHz and 3600MHz frequency bands (as amended).

4 For the details, see: https://smc.gouvernement.lu/fr/actualites/articles/2020/Detail5G.html

5 Commission Implementing Decision (EU) 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use in the Union; Commission Implementing Decision (EU) 2019/235 of 24 January 2019 on amending Decision 2008/411/EC as regards an update of relevant technical conditions applicable to the 3400-3800 MHz frequency band.

Draft Law implementing the European Electronic Communications Code in Luxembourg

What happened?

On July 16 2020, the Luxembourg Minister of Communications and Medias presented

draft Law No. 7632 on the European Electronic Communications Code (the " **Draft Law**") to the Chamber of Deputies. The Draft Law aims at implementing into Luxembourg law the Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (the "**EECC Directive**")[1].

What is it about?

The EECC Directive aims to harmonise the regulation of electronic communications networks, electronic communications services and associated facilities and services through the European Union. It also outlines the tasks incumbent on the national regulatory authorities (in Luxembourg, the *Institut Luxembourgeois de Régulation*). At national level, the Draft Law implementing the EECC Directive intends to repeal and replace the amended Law of 27 February 2011 on networks and electronic communications services while keeping some of the specific provisions which do not derive from or are not affected by European law.

What are the main expected innovations?

As new features, the EECC Directive and the Draft Law:

- Extend the legislative scope of electronic communications to non-numbering-based interpersonal communications services, the **over-the-top services** (the **"OTTs"**). Messaging services such as Apple iMessage, WhatsApp, Facebook Messenger, Webmail services (e.g. Gmail) or voice/video calls such as FaceTime or Skype are now within the scope of the legislation and **may be subject to *ex ante* supervision**. Like any other provider of communications services, OTTs will be required to provide information to the *Institut Luxembourgeois de Régulation*, be subject to security audits and be subject to investigations in the event of non-compliance.
- Aims at progressively reducing *ex ante* regulation of dominant operators as competition intensifies to create **effective and sustainable competition** with a positive impact on prices, quality and choice for end-users.
- Promote the **deployment of very high-capacity** communications networks by granting to the electronic communications operators a right to access all public physical infrastructure, including street furniture such as street lights, street signs, traffic lights, billboards, bus and tramway stops.
- Prohibit any unnecessary restrictions on the interconnection of access points to local wireless networks allowing the **sharing of private WiFi**.
- Harmonise radio spectrum management for electronic communications networks and services and impose the release of the frequency bands needed for the

deployment of the 5G technology at the latest on 31 December 2020.

- Promote access to high speed internet at an affordable price as a **universal service**.
- Harmonise and **strengthen consumers' rights** by requiring operators to provide specific information to consumers prior to entering into a contract.

Additional Luxembourg specificities provided by the Draft Law

The Draft Law extends the obligations of the EECC Directive to impose additional obligations on electronic communications operators.

Article 42 of the Draft Law concerning the security of networks and services provides for **an obligation to notify** the *Institut Luxembourgeois de Régulation* "without delay" of the technical and organisational security measures implemented. This requirement is not imposed by the EECC Directive, but already exists under Luxembourg law for the providers of public electronic communications networks and electronic communications services available to the public.

Article 114(3) of the Draft Law lists the main elements of information required to be contained in the contract summary to be provided to the consumer before entering into the contract. In the event that the contract summary cannot be provided at that time, the Draft Law provides that the contract will take effect after the consumer agrees "in writing or on any other durable medium" after having been provided with the contract summary. The requirement to obtain the agreement of the consumer "in writing or on any other durable medium" is not expressly imposed by Article 102 of the EECC Directive and constitutes an additional obligation in the Draft Law.

What's next?

The Luxembourg Draft Law is currently being discussed at the Chamber of Deputies as part of the legislative procedure. It is subject to potential amendments to take into account the upcoming opinions of the Council of State and other institutions. Consequently, the final law to be adopted may deviate from the Draft Law in its legal provisions. Depending on the pace of the legislative process, we do not exclude that that the law may be adopted by year end or shortly after.

This may also interest you :

- 5G: Opportunities and Legal Challenges - Part 2. Deployment of 5G in Luxembourg
- 5G: Opportunities and Legal Challenges

1 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, which is a recast of the 2002 Telecom Package including the (i) Access Directive 2002/19/EC; (ii) Authorisation Directive 2002/20/EC; (iii) Framework Directive 2002/21/EC; and (iv) Universal Service Directive 2002/22/EC.