ELVINGER HOSS PRUSSEN

ELVINGER HOSS LUXEMBOURG LAW

ICT, IP, media and data protection NEWS

TABLE OF CONTENTS

5G: Opportunities and Legal Challenges

Part 1. Overview of 5G technology opportunities

This article is the first of a series of following publications, which will focus on more specific 5G topics.

*Register **here** to follow our series of articles on the theme of 5G over the next month.*

What is 5G?

5G is the 5th generation of wireless technology that will considerably improve the current framework of telecommunications based on the existing 4G. It is expected to be one of the fastest wireless technologies ever created. It will allow the emergence of new services, applications and capabilities. It will have a particular impact on the ISP's business model and their offer of services thanks to the so-called "network slicing" technology, which will enable them to virtualise "slices" of the network and provide services specifically tailored and continually scalable to the needs of each users. Last but not least, it will enable technologies which will facilitate network management and reduce costs considerably. The 5G technology is expected to be deployed by the end of this year in Luxembourg in accordance with the European roadmap aiming to make 5G available in at least one city per Member State by 2020.

What will change?

More than simply enhancing the mobile broadband (i.e. speed of data transfers in bits/s), 5G allows the use of applications requiring ultra-reliable and low latency connections (i.e. the delay between a command and its execution) and pave solid steps for the development of the Internet of Things ("IoT") industry. The opportunities foreseen include, in particular, autonomous driving and car-to-car real-time communications (e.g. detection of traffic jams or accidents and alerting other drivers on the way), road traffic management, smart homes, smart cities, remote surgery, remote surveillance and maintenance of industrial machines, etc.

What can 5G be used for?

At least 3 different usage scenarios of 5G have been identified together with their specific technical requirements:

- Enhanced mobile broadband i.e. greater bandwidth and support of more connected devices ("eMBB"): eMBB is an extension to existing 4G technology and addresses the applications supporting a small number of devices (compared to MMTC – see below), each of which requires high bandwidth (5G's data rate is up to 20Gbps downlink), such as augmented reality, virtual reality, and other services requiring mobility, low latency, high data rate and wide area coverage. It will also support the growing data traffic needs (e.g. 3D video, 4K video transmission, streaming services, UHD screens, etc.).
- Ultra-reliable and low latency communications ("UR-LLC"): UR-LLC addresses applications with strict requirements for specifications such as low latency (5G provides 1ms latency, compared to 20ms for 4G), high reliability, security and throughput (self-driving and car-to-car communications, remote surgery, public safety services, operation of mining, oil and pipelines, etc.)
- Massive machine-type communications "(mMTC"): mMTC refers to networks supporting a large number of devices (i.e. about 10^6 devices/km^2) requiring low bandwidth connectivity as they receive and transmit short packets. Such devices typically do not need low latency while security and resilience are essential to their functions (e.g. smart homes, smart cities, smart industries, etc.)

What impact will it have on society?

The 5G technology will affect a large part of our society in many different ways, including social, industrial, medical, environmental, financial and economic activities. It reveals new challenges from a legal and regulatory perspective both in relation to the deployment of this technology (e.g. allocation of spectrum, installation of antennas, administrative authorisation, access to public infrastructures, network security, etc.), with the development of new activities based on this technology (e.g. automation, digitalisation), and in relation to the day-to-day use of this technology (related criminal and civil responsibility, privacy and data protection, etc.).

Is there a legal framework covering 5G?

5G is covered in various aspects by several Luxembourg laws and European Regulations, in particular the Law of 27 February 2011 on network and electronic communication services (as amended)[1], the Law of 30 May 2005 on the management of radio waves (as amended), the Law of 30 May 2005 on the

protection of persons in relation to the processing of personal data in the sector of electronic communications (as amended) (e-Privacy law), Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), the Law of 28 May 2019 concerning measures for a high common level of security of network and information systems (NIS Law), and the Law of 23 October 2011 on competition (as amended). As regards the "network slicing" technology, particular concerns have also been raised in relation to Regulation (EU) 2015/2120 laying down measures concerning open internet access, which aims to ensure an equal and non-discriminatory treatment of internet traffic (net neutrality).

Are there other related laws and regulations?

Other legislation at European and Luxembourg level also apply in relation to the deployment of and investments in the 5G infrastructures and technologies, which are not covered in this overview, such as Regulation (EU) 2018/1971 establishing the Body of European Regulators for Electronic Communications (BEREC), Regulation (EU) 531/2012 on roaming on public mobile communications networks in the Union, Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment, transposed in Luxembourg by the Law of 27 June 2016, Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks, transposed in Luxembourg notably by the Law of 22 March 2017 and the Law of 24 May 2011 on services in the internal market, Directive 2014/24/EU on public procurement, transposed in Luxembourg by the Law of 8 April 2018, Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, Regulation (EC) 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, Regulation (EU) 2016/1036 on protection against dumped imports from countries not members of the European Union, Regulation (EU) 2016/1037 on protection against subsidised imports from countries not members of the European Union, Regulation (EU) 2015/478 on common rules for imports, etc..

Read our next publication

In our next publication dedicated to the 5G theme, we will cover matters related to the allocation of part of the spectrum to the 4 Luxembourg telecom operators who won the auction organised by the *Institut Luxembourgeois de Régulation* ("ILR"), as well as their rights and obligations resulting from the licences that they obtained, and the effective deployment of 5G technology in Luxembourg.

> 1. The applicable Law of 27 February 2011 will be repealed and replaced by a new law (Bill of law No. 7632 currently being discussed at the Chamber of Deputies) transposing the Directive (EU) 2018/1972 establishing the European Electronic Communications Code, which is a recast of the 2002 Telecoms Package including the (i) Framework Directive 2002/21/EC; (ii) Access Directive 2002/19/EC; (iii) Authorisation Directive 2002/20/EC; and (iv) Universal Service Directive 2002/22/EC.

EDPB's FAQ about the invalidation of the Privacy Shield

What happened?

On 23 July 2020, the European Data Protection Board ("**EDPB**") released **a set of questions** (the "**FAQ**") posed by European supervisory authorities regarding the implications of **Case C-311/18, Data Protection**

Commissioner v Facebook Ireland and Maximillian Schrems ("**Schrems II** ") ruled on 16 July 2020 by the Court of Justice of the European Union ("**CJEU**").

What happened previously ?

In the Schrems II ruling, the CJEU invalidated the EU-U.S. Privacy Shield Framework, which allowed personal data transfers to more than 5,000 data recipients located in the United States of America ("**U.S.**"). The CJEU ruled that the Privacy Shield did not provide data protection standards essentially equivalent to those required under EU law, in particular under the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"). (**click here to see our publication**)

The CJEU also confirmed that the EU standard contractual clauses ("**SCCs**"), which are in practice commonly used for transferring personal data outside of the European Economic Area ("**EEA**"), are valid *per se*. However, that validity depends on whether the requirements of the data recipient's domestic law results in limitation of personal data protection, which must remain compatible with EU law. As regards the U.S. law in particular, the CJUE considered that surveillance programmes enabling the U.S. authorities to access personal data for national security purposes contravene the principle of necessity and proportionality under EU law as such programmes do not provide for any limitations to the power of U.S. authorities. U.S. law also does not grant data subjects with actionable rights against the US authorities as under the EU law.

What are the key takeaways?

While the U.S. Department of Commerce and the EU Commission have initiated discussions on the possibility to enhance the Privacy Shield to comply with the CJUE judgment, the EDPB is currently assessing the impact on personal data transfers to the U.S. and the alternative solutions in the light of EU law. Meanwhile, the FAQ is intended to provide some clarity on the most pressing questions in relation to this matter:

- **Data transfers based on the EU-U.S. Privacy Shield.** Because of the invalidity of the EU-U.S. Privacy Shield, the latter is no longer a valid mechanism for the transfer of personal data to the U.S. in accordance with EU law. Accordingly, EEA data exporters and importers must opt for an alternative transfer mechanism.
- **No grace period.** The EDPB also clarified that the Schrems II ruling does not provide for any grace period. Data transfers operated via the EU-U.S. Privacy Shield are considered non-compliant with existing data protection law with immediate effect. In practice, however, it is expected that the EU supervisory authorities remain provisionally flexible as regards the validity of the legal bases used for personal data transfers to the U.S., but there is no common position as of today between the different supervisory authorities on this matter.
- **The responsibility of the data exporters and data importers when using SCCs.** With the invalidation of the EU-U.S.-Privacy Shield, the CJUE found that existing data protection standards in the U.S. are not sufficient to be considered as essentially equivalent to those of UE law. As a consequence, each data exporter and data importer should collaborate to operate an assessment, taking into account the circumstances of the personal data transfers, the requirements of the U.S. law and any supplementary measures that they could put in place on a case-by-case basis to ensure that U.S. law does not impinge on the adequate level of protection guaranteed by the SCCs. In the event that the result from such an assessment is that an adequate level of data protection cannot be ensured, the data transfers should immediately be suspended or notified to the competent supervisory authority (i.e. in Luxembourg, the CNPD).

- **The nature of the supplementary measures.** The EDPB underlined that it is currently assessing the type of supplementary measures that could be implemented in addition to SCCs, whether legal, technical or organisational measures, where the SCCs will not provide a sufficient level of data protection on their own. The EDPB should provide further guidance in this respect.
- **EEA to U.S. data transfers on the basis of derogations foreseen in Article 49 GDPR.** As the EDPB underlines, another existing legal basis for personal data transfers to the U.S. consist in the derogations listed under Article 49 GDPR, which are of restrictive interpretation and may be considered only in the absence of adequacy decision and other appropriate safeguards. Such derogations may be relied on if the conditions set forth in this Article apply and in accordance with the interpretation of the EDPB issued in this respect (see **here**). However, such derogations do not constitute appropriate legal bases for personal data transfers taking place on a large scale and in a systematic manner. In particular, where relying on the necessity of the transfer for the performance of a contract, any such transfer must remain occasional. As regards the consent of the data subjects, this consent should be explicit, specific for each data transfer and adequately informed.
- **Data transfers to third countries other than the U.S.** The CJEU ruling specifically addressed personal data transfers to the U.S. However, the rules set out by the CJEU apply to the same extent to any other third country. Data exporters and importers are required to assess whether the domestic law of the recipient countries allow them to comply in practice with EU law when implementing the SCCs. If not, any supplementary measures, which are not impinged upon by the recipient's domestic law in practice, should be considered as ensuring an essentially equivalent level of data protection as provided in the EEA.

Further points of attention

In conclusion, there is currently no real alternative to the use of the EU-U.S. Privacy Shield and SCCs for transferring personal data to the U.S., unless appropriate supplementary measures could be combined with the SCCs to ensure an essentially equivalent level of data protection. However, there is no guidance as to the consistence of such supplementary measures. Relying on the derogations listed under Article 49 GDPR (i.e. consent, performance of a contract, public interest, etc.) is only appropriate in exceptional circumstances in accordance with the interpretation of the EDBP and cannot cover personal data transfers taking place on a large scale and in a systematic manner.

We will keep you posted about any further guidance or developments in this respect.

EDPB's updated Guidelines on consent under GDPR: cookies and scrolling

What happened?

On 10 April 2018, the Article 29 Working Party adopted its **Guidelines on consent under Regulation 2016/679** (the "**GDPR**"), which were endorsed by the European Data Protection Board (the "**EDPB**"). These Guidelines provide clarifications and examples for obtaining valid consent under the GDPR.

What's new?

On 4 May 2020, the EDPB adopted **an updated version of those Guidelines** revising certain

recommendations while the rest of the document was left unchanged, except for some editorial modifications. This version of the Guidelines supersedes the version adopted in April 2018.

Key takeaways to consider.

The EDPB provided additional guidance to clarify the sections of the Guidelines concerning the "Conditionality" of consent and the "Unambiguous indications of wishes" with regard to:

- the validity of consent of data subjects interacting with so-called "cookie walls" on websites;
- the process of scrolling on a Web page to consent.

In more detail.

The EDPB wishes to emphasise the fact that access to a service cannot be conditional upon the consent for processing personal data (where such processing is not necessary to provide the service concerned): "*access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user*". To illustrate this principle, the EDPB uses the example of "cookie walls" that prevent users from accessing a website unless they accept cookies. According to the EDPB, such cookie wall mechanisms are not compliant with the GDPR as they do not provide a genuine choice to the data subjects so that the consent cannot be considered as freely given and is thus invalid.

Furthermore, the EDPB states that "*actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action*". This means that cookie banners stating that any further browsing will be considered as an acceptance for the deposit of cookies are not compliant with the GDPR, as that they do not satisfy the requirement of an unambiguous indication of wishes.

The clarifications provided by the EDPB in the new Guidelines shall be read in conjunction with the ruling of the Court of Justice of the European Union in the **"Planet 49" case**, which concluded that a pre-checked box that users must deselect to refuse the storage of cookies on their terminal equipment is not valid consent.

Based on the foregoing, online business operators must ensure that any and all data subjects are provided with a genuine choice to accept or to decline the use of cookies without detriment while access to their service shall not be made conditional on the data subject's consent to the storage of cookies in the event that such cookies storage is not strictly necessary for using the service.

Further points of attention

The aforementioned should also be considered in the light of the provisions of **Directive 2009/136/EC** ("ePrivacy Directive") which governs the use of cookies. The ePrivacy Directive requires consent from the user, if a website uses cookies. With some exceptions, such consent relating to the processing of personal data shall comply with the requirements for valid consent under the GDPR. That is why cookie walls have been analysed from that standpoint by the GDPR.

Do intermediaries have the obligation to provide the email address of alleged counterfeiters?

What happened?

On 9 July 2020, the CJEU ruled **Case-264/19 Constantin Film Verleih GmbH v YouTube LLC and Google Inc.**. This case provides an important clarification on the duties of hosting service providers where their users are accused of infringing copyright by uploading protected video materials.

What is the applicable rule at stake?

Under Article 8 of **Directive 2004/48/EC** on the enforcement of intellectual property rights, hosting service providers may be obliged, where proportionate and requested by a judicial authority, to disclose the "names and addresses" of the alleged counterfeiter(s), including the listed persons (i.e. the manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers).

What's new?

The dispute in the case at hand focused on the notion of "address" and whether it includes the email address, the telephone number and IP address used to upload content. Indeed, YouTube could not disclose the names and addresses of the user(s) concerned, as such information was not in its possession. The users' real names and postal addresses are in fact not required by the platform to create an account and upload content online.

The CJEU held that the term "address" must be interpreted as referring only to the postal addresses of the alleged infringer(s). As a result, YouTube was not required to disclose the email addresses, the IP addresses or any telephone numbers of the user(s) concerned.

In more detail

To arrive at that decision, the court gave the following reasoning:

- The CJEU observed that Directive 2004/48/EC does not define the term "address" and neither does it refer to the laws of Member States to determine its meaning. Therefore, the CJUE considered that it was an autonomous notion under the European Union and that its meaning and scope must be determined in accordance with its usual meaning in the common language, which exclusively covers the postal address;
- In the absence of a definition within Directive 2004/48/EC, the preparatory work leading to its adoption failed to contain anything to suggest that the notion of "address" should be understood to include anything more than the postal address;
- Finally, the CJEU examined other EU legal acts referring to email addresses or IP addresses. None of them uses the term "address" without further clarification to designate a telephone number, email or IP address.

In the case at hand, the measures provided under Directive 2004/48/EC were not sufficient to allow the claimant to identify the alleged counterfeiter(s). However, the CJEU restated the ability for Member States to provide in their national law that judicial authorities may order more extensive disclosures of information. In the absence of any extended disclosure requirement under a given national law, copyright holders may only request the names and (postal) addresses as identification information of the persons concerned. In Luxembourg, the same disclosure requirements have been transposed into national laws to reflect the provisions of Directive 2004/48/EC. Accordingly, the disclosure obligations under Luxembourg law are also limited to the names and (postal) addresses of the concerned persons.

Online platforms: storing infringing products on behalf of third parties does not constitute trademark use

On 2 April 2020, the Court of Justice of the European Union ("CJEU") rendered a judgment[1] in a dispute between companies of the Amazon group and Coty Germany GmbH ("Coty"), a distributor of perfumes that holds a licence for the EU trademark "Davidoff", registered for perfumes, essential oils and cosmetics.

Coty initiated proceedings in Germany against four companies of the Amazon group alleging that these companies committed a trademark infringement by storing Davidoff perfume bottles in Amazon warehouses that were subsequently sold, without Coty's authorisation, on the Amazon online marketplace by third-party sellers through the "Fulfilment by Amazon" scheme. Indeed, through this scheme, Amazon offers, in particular, the possibility for third-party sellers to make use of Amazon's warehouses subject to the payment of a fee. It should be noted that the trademark rights on the perfume bottles concerned were not exhausted, that is, Coty had not previously put those perfume bottles on the European Union market

The first courts in Germany dismissed the action brought by Coty and the Federal Court of Justice (Germany) decided to stay the proceedings and refer the following question to the CJEU for a preliminary ruling: "*Does a person who, on behalf of a third party, stores goods which infringe trade mark rights, without having knowledge of that infringement, stocks those goods for the purpose of offering them or putting them on the market, if it is not that person himself but rather the third party alone which intends to offer the goods or put them on the market?*"

The CJEU responded negatively and underlined that such a storage operation does not constitute a "trademark use" pursuant to the EU regulation on the European Union trademark[2] (the "EU Trademark Regulation"), since Amazon had not itself offered the perfume bottles for sale or put them on the market and did not intend to do so. Similarly, Amazon did not itself use the sign in its own commercial communications.

Pursuant to the EU Trademark Regulation, the use of a trademark is subject to the prior authorisation of the holder of the trademark rights. However, in the absence of trademark use, Amazon cannot be found liable for infringement of the trademark rights over the sign "Davidoff".

The CJEU reiterated that the liability of an economic operator in relation to a trademark use may be assessed in light of other provisions such as the Directive on electronic commerce[3] or the Directive on the enforcement of intellectual property rights[4]. However, in the case at hand, the question submitted to the CJEU was worded in a narrow way thus giving the possibility for the CJEU not to pursue its analysis.

If this ruling covers an interesting point and was greeted with relief by online platforms, its concrete impact on online platforms must not be exaggerated. It is only limited to the storing of goods infringing trademark rights by a person on behalf of third parties, that person not being aware of the infringement. There is little doubt that the broader role of online platforms such as Amazon (advertising sale offers by

third parties on the online platform, handling return of defective products, managing the payment process, etc.) in the sale of goods by third-party sellers would be emphasised by the referring courts in future proceedings.

1. Case C-567/18 Coty Germany GmbH v Amazon Services Europe Sàrl, Amazon Europe Core Sàrl, Amazon FC Graben GmbH and Amazon EU Sàrl.
2. The provisions in question are specifically Article 9(2)(b) of Council Regulation (EC) No 207/2009 of 26 February 2009 on the European Union trade mark and Article 9(3)(b) of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark.
3. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
4. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.