ELVINGER HOSS PRUSSEN

ELVINGER HOSS
LUXEMBOURG LAW

ICT, IP, media and data protection NEWS

TABLE OF CONTENTS

The use of mobile applications in the fight against COVID-19 – Guidelines from the EDPB

The situation around the COVID-19 pandemic enters into a new stage. De-confinement measures are being adopted and general travel restrictions are gradually lifted. As a result, certain governments tend to use modern technologies in order to track the effects of the adopted strategies, to contain the spread of the virus, and to prevent and mitigate possible second waves of the virus. An important tool in this process is the use of mobile contact tracing applications ("**COVID-19 Applications**") dedicated to recognising individuals who have been in contact with virus carriers to allow a rapid interruption of contamination chains.

While Luxembourg has not so far made the choice of the use of a Covid-19 Application and has only implemented a "remote monitoring of all patients who test positive for COVID-19 (both those who are in isolation at home and those who have just been discharged from hospital)" on a voluntary basis,[1] France and Italy have already released their COVID-19 Applications, *StopCOVID* and *Immuni,* respectively.

COVID-19 Applications obviously require compliance with European data protection standards, particularly the EU General Data Protection Regulation[2] ("**GDPR**"). European institutions have advocated a coordinated approach and the European Data Protection Board ("**EDPB**") issued its guidelines[3] on April 21, 2020 regarding the rules that shall govern COVID-19 Applications, such as the following:

- **The requirement of a Data Protection Impact Assessment ("DPIA").** While contact-tracing applications are likely to result in a high risk to the rights and freedoms of natural persons, the EDPB considers that a DPIA must be carried out before the implementation of a COVID-19 Application.
- **Lawful bases of processing.** The EDPB underlines that the use of COVID-19 Applications must rely on a strict voluntary basis (no one shall be obliged to upload a COVID-19 Application) and that users must remain in absolute control over their own personal data. The EDPB notes that this does not necessarily imply that the processing of personal data will be based on consent.Other lawful bases for processing are available, such as the necessity for the performance of a task carried out in the public interest[4]. Regarding health data[5] (such as the status of an infected person), their processing shall rely either on explicit consent from the data subject or on a specific lawful basis such as the necessity for reasons of public interest in the area of public health[6] or for scientific research purposes or statistical purposes.[7]
- **The use of proximity data rather than location data.** The EDPB underlines that COVID-19 applications should not involve the use of location data, but only process proximity information, which is obtained without locating individuals.
- **COVID-19 Applications as a complementary tool to manual contact tracing.** COVID-19 Applications should be understood as complementary to manual contact tracing already performed by qualified personnel who are able to evaluate virus transmission chains and respond accordingly. The EDPB therefore recommends that advice and recommendations sent to users should not be based on solely automated processing.
- **Erasure of data.** The EDPB recommends that all personal data should be erased or anonymised as soon as the pandemic is over. Personal data should only be kept for the duration of the COVID-19 crisis.

The coming months will show whether the COVID-19 Applications reveal themselves compliant with these rules, and as an effective response to control and mitigate the rise of the virus infections. Any such strategy must always be guided by existing data protection principles in order to ensure the respect of the individual rights and freedoms of the data subject.

> 1. **Press release from the Ministry of Health of 9 April 2020 on the MAELA telemonitoring tool** .
> 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
> 3. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID 19 outbreak: **EDPB Guidelines 04/20**.
> 4. Article 6.1 (e) GDPR.
> 5. Health data qualify as "special category of personal data" (i.e sensitive personal data) under the GDPR.
> 6. Article 9.2 (i) GDPR.
> 7. Article 9.2 (j) GDPR.

EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

Important scientific research efforts are currently being made in order to provide rapid research results in the fight against the COVID-19 pandemic. This involves the processing of health data of many individuals. In its Guidelines adopted on 21 April 2020[1], the European Data Protection Board ("**EDPB**") addresses

relevant legal questions concerning the use of health data for scientific research purposes in light of the General Data Protection Regulation ("**GDPR**")[2] such as the legal basis, the rights of the data subjects including the right of information, data protection principles and international data transfers for scientific research purposes.

The EDPB underlines that several provisions of the GDPR govern the use of personal data for scientific research purposes and that those provisions shall of course apply in the Covid-19 context. For example, the GDPR provides a derogation from the prohibition of processing sensitive data such as health data (referred to as a "special category of personal data" under the GDPR) where it is necessary for scientific research purposes.

The EDPB points out that the processing of health data for scientific research purposes refers to two types of processing: (i) "primary use" where health data is directly collected for the purpose of scientific studies (in the case of clinical trials on individuals suspected of being infected) and (ii) "secondary use" where health data initially collected for another purpose (as part of a medical consultation, for example) are further processed for scientific research purposes. The above distinction has implications on the other obligations set out in the GDPR.

The EDPB also recommends the use of anonymised data (i.e.where no one can refer back to data subjects, as opposed to pseudonymised data) whenever possible and to define proportionate and adequate storage periods (the length and the purpose of the scientific research can serve as criteria to set storage periods).

> 1. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak: **EDPB Guidelines 03/2020**.
> 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

The implementation of the Shared Medical Record in Luxembourg (dossier de soins partagé) : data protection aspects to consider

On 1 January 2020, the Grand Ducal Regulation of 6 December 2019 specifying the terms and conditions for setting up the shared medical record[1] (the "**Grand Ducal Regulation**") entered into force, thus implementing the *dossier de soins partagé* (the "**Shared Medical Record**"). The Shared Medical Record is deployed by the eSanté Agency, an economic interest group encompassing the Luxembourg State, the *Caisse nationale de santé* (national health insurance provider) and the *Centre commun de la sécurité sociale* (one of the social security institutions), as well as representative bodies for health care providers and associations representing the interests of patients. The Shared Medical Record is intended to provide a more efficient follow-up of the health data of patients in Luxembourg by keeping their medical history available to both the patient himself, as well as to the health professionals.

The sensitive nature of the personal data contained within the Shared Medical Record obviously calls for adequate data protection, confidentiality and security standards. As a consequence, the *Commission nationale pour la protection des données* ("**CNPD**") was largely involved in the elaboration process and has rendered opinions[2] regarding the compliance of the Shared Medical Record with existing data protection legislation, in particular the General Data Protection Regulation[3] ("**GDPR**").

We draw your attention to the following:

- **The definition of health professionals**. The Grand Ducal Regulation defines health professionals as

any natural person lawfully exercising a regulated health profession and any health professional, any hospital establishment, and any health care provider lawfully exercising their profession outside the hospital sector referred to in the Social Security Code[4] (such as medical analyses laboratories, pharmacies, opticians).

- **Objection and access rights to the Shared Medical Record by the holder.** If the holder does not object to the creation of the Shared Medical Record, it will be automatically activated 30 days after receipt of the letter from the eSanté Agency informing the holder of its creation. Health professionals may then access the Shared Medical Record. The holder may modify access rights and deny one or more health professional(s) access to their entire file or render certain data inaccessible to one or more health professional(s). The processing of personal data by the eSanté Agency in relation to the Shared Medical Record relies on specific provisions of the Social Security Code[5].

- **Recipients**. Recipients of the Shared Medical Record are the patient and any health professional related to the patient. The CNPD recommended in its opinion that the Grand Ducal Regulation expressly clarifies that recipients shall not be extended in the future to other categories of natural and legal persons (such as private insurance companies, employers, medical practitioners acting as experts on behalf of third parties, etc.). This recommendation has not, however, been taken into account in the final version of the Grand Ducal Regulation.

- **Joint controllership.** Both the Grand Ducal Regulation as well as the Social Security Code[6] provide that the eSanté Agency is responsible for the processing of personal data contained in the Shared Medical Record. The CNPD questioned this sole controllership, stressing that the eSanté Agency on the one hand and the health professionals on the other hand, jointly participate in achieving the purposes and means of the processing of personal data contained in the Shared Medical Record. In the CNPD's view, the eSanté Agency and the health professionals act in practice as joint controllers. The CNPD analysis was partly taken into account since the final version of the Grand Ducal Regulation refers to the health professionals in their capacity as controllers of the personal data they process in the context of the Shared Medical Record (for example, when they enter information regarding a patient's illness or results of medical analysis directly in the relevant Shared Medical Record). It must be noted that the legal basis relied upon by the health professionals for processing such health data is not clear.

- **Data retention and data subject rights.** The holder of a Shared Medical Record may close his Shared Medical Record at any time via the website or upon request addressed to the eSanté Agency. Within 10 years following the closing of the Shared Medical Record, the holder may reopen it, without losing the data contained therein. However, if not reopened within the period, the data contained in the Shared Medical Record shall be deleted 10 years after its closure. From the date of closure, the personal data contained in the Shared Medical Record are archived and rendered inaccessible. The Shared Medical Record will also be closed after 10 years of inactivity from the latest access. The patient benefits from the right to erasure or the right to rectify inaccurate or incomplete data. Those rights shall be performed by the health professional or the eSanté Agency.

- **Data Security.** The health professionals, in their capacity as data controllers, shall implement appropriate technical and organisational security measures to ensure a level of security appropriate to the risks.

In conclusion, the Shared Medical Record is without doubt an ambitious step towards a more efficient and modern health care service in Luxembourg. It remains to be seen and verified if the data protection standards implemented for this eHealth tool (in particular the technical and organisational security measures) are high enough to encourage the population to trust and adhere to it.

1. Règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé. **http://legilux.public.lu/eli/etat/leg/rgd/2019/12/06/a909/jo**
2. This article focuses on the additional opinion rendered by the CNPD on October 18, 2019 (Deliberation n° 51/2019): **https://cnpd.public.lu/dam-assets/fr/decisions-avis/2019/51-DSP.pdf**
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
4. See Article 61 (2) of the Social Security Code.
5. Articles 60*ter* and 60*quater*.
6. Article 60ter paragraph (4) of the Social Security Code.

Breach of software licence in relation to IP rights and availability of the infringement action: a welcome clarification from the CJEU

Following a request for a preliminary ruling from the Court of Appeal of Paris (France), the Court of Justice of the European Union (the "CJEU") clarified, in a judgment of 18 December 2019[1], that the violation of a clause of a software licence agreement relating to intellectual property rights shall be treated as an "*infringement of intellectual property rights*" within the meaning of Directive 2004/48/EC[2] (the "Enforcement Directive") which implies that the holder of the author's rights (economic rights) over such software must be able to benefit from the guarantees provided for by the Enforcement Directive (which includes the infringement action).

This ruling should put an end to a trend resulting from certain national court decisions[3] in which it was judged that a breach of a software licence agreement relating to intellectual property rights could not lead to the engagement of tortious liability (*responsabilité délictuelle*) and, therefore, that the infringement action was not the appropriate action for a right-holder to initiate before the courts when facing a violation of the terms of a software licence agreement by a counterparty.

In the case at hand, the software publishing company, IT Development, had granted a licence to the telephone operator, Free Mobile, for the use of a software package. Considering that Free Mobile had modified the source code of its software in breach of the licence agreement, the software publisher brought an action against Free Mobile for infringement (under French law, author's rights infringement is based on tortious liability). In line with the case law mentioned above, the first judges declared the claims brought by IT Development based on Free Mobile's tortious liability inadmissible. According to them, the software publisher company should have initiated an action for contractual liability.

For the Court of Appeal of Paris, the question was not so straightforward. On the one hand, the Court of Appeal acknowledged the existence of the principle of non-cumulation under French law according to which (i) one person cannot hold another person liable in contract and tort for the same acts, and (ii) tortious liability is excluded in favour of contractual liability where the damage suffered by one of those persons results from non-performance or improper performance of a contractual obligation. On the other hand, the Court of Appeal underlines that the French rules regarding the infringement action do not refer to the existence or the absence of a contract between the parties and do not differ depending on whether or not such a contract exists.

In light of this, the Court of Appeal decided to stay the proceedings and refer to the CJEU for a preliminary ruling. The question[4] was whether the "Enforcement Directive" and Directive 2009/24/EC[5] (the "Software Directive") "*must be interpreted as meaning that the breach of a clause in a licence agreement for a computer program relating to the intellectual property rights of the owner of the copyright of that program falls within the concept of 'infringement of intellectual property rights', within the meaning of the [Enforcement Directive], and that, therefore, that owner must be able to benefit from*

the guarantees provided for by that directive, regardless of the liability regime applicable under national law".

This is a crucial issue as the calculation of the financial compensation will be different depending on the liability regime invoked. Indeed, pursuant to the civil liability regime (tortious liability), the claimants shall obtain full reparation of their damage. Liability caps or limitations that would be provided for by a clause of a software licence agreement would not apply[6]. Moreover, the rules governing jurisdiction, the evidence that are available or the statutes of limitation may differ depending on the liability sought by the claimant (tortious liability or contract liability).

Responding positively to the question referred to it, the CJEU points out that the Software Directive does grant the right-holder the exclusive right to authorise or prohibit the modification of a software (in particular the adaptation or transformation of the source code) and does not make such protection dependent on whether or not the alleged violation of rights is a breach of a licence agreement.

Moreover, the CJEU underlines that the Enforcement Directive specifies that it applies to *"any infringement of intellectual property rights*"[7] which shows that a breach of a contractual clause relating to the exploitation of an intellectual property right shall also be covered. The CJEU has thus clarified that the right-holder that entered into a licence agreement with a third party is entitled as any other holder of intellectual property rights to benefit from and use the measures, procedures and remedies set out in the Enforcement Directive (including the infringement action).

This ruling from the CJEU shall be approved, as the approach taken is fair and in line with the directives mentioned above. A holder of intellectual property rights shall not be disadvantaged only because it took the decision to organise contractually the exploitation of its intellectual property rights.

It is interesting to note that the CJEU does not rule on the nature of the liability regime that shall apply in the event of a violation of author's rights (economic rights) over a software by a licensee. The CJEU states on the contrary that such determination falls within the competence of the Member States. However, the Member States will not have much room for manoeuvre, as the liability regime applicable shall not imperil the effective protection granted to the holder of author's rights (economic rights) over a software by the Enforcement Directive and the Software Directive.

1. Case C-666/18, IT Development SAS v. Free Mobile SAS.
2. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
3. This trend in case law was identified in France. In Luxembourg, the *Tribunal d'arrondissement* declared admissible an infringement action based on the violation of certain provisions of the Law of 18 April 2001 on the author's rights, related rights and databases, as amended initiated by the owner of author's rights over a software against its counterparty even though the parties were bound by a licence agreement. The claimant, however, did not invoke a violation of a specific clause of the licence agreement. In this case, the law of the licence agreement (the laws of the State of Pennsylvania in the United States of America) was disregarded. The Luxembourg judges indicated that the law chosen by the parties to govern their contractual relationships regarding the sale of software licences to third parties shall not govern the action for damages arisen out of author's rights infringement, which are purely tort actions. They confirmed that the Luxembourg law (i.e the law of the country in which the protection is sought) shall apply to the case (Civil Judgement No. 49/2014 (8th chamber), 4 March 2014). This was confirmed by the Court of Appeal in a decision of 30 March 2017 (No 41358).
4. The question was reformulated by the CJEU.
5. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.
6. It is true however that the parties to a licence agreement/Software as a Service Agreement (SaaS) commonly accept not to limit their liability to the other party in the event of author's rights infringement (provided that

certain conditions are complied with).

7. Article 2(1) of the Enforcement Directive.

For any further information please contact us or visit our website at **www.elvingerhoss.lu**.

The information contained herein is not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific legal advice concerning particular situations.

We undertake no responsibility to notify any change in law or practice after the date of this newsletter.