ELVINGER HOSS PRUSSEN

ELVINGER HOSS LUXEMBOURG LAW

ICT, IP, media and data protection NEWS

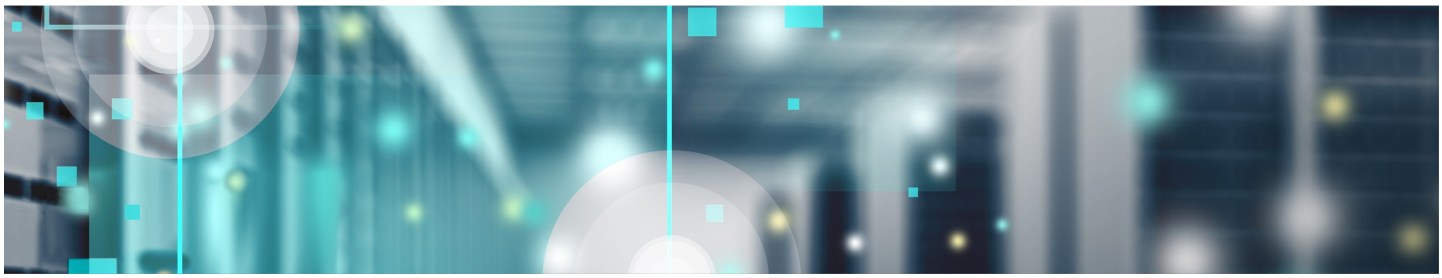


TABLE OF CONTENTS

Luxembourg law recognises issuance of dematerialised securities in blockchains

Artificial Intelligence: the Commission's Regulation Proposal and AI strategy in Luxembourg

The Data Governance Act - regulating access to data held by public authorities

The impact of the Brexit deal on personal data transfers from the EU to the UK

GDPR - Adequacy decisions for the UK

ePrivacy Regulation: The return?

GDPR - Transfers of personal data in the UCI world after Schrems II

Regulating access to Open Data - free access to data held by public bodies

Focus on European Commission's proposal for a Digital Services Act

GDPR in the health research sector: EDPB response to EU Commission on a consistent application

Guidelines regarding the geolocation of vehicles made available to employees

Digital Green Pass: EU data protection authorities' position

GDPR anniversary - Time to take your business for a data protection compliance check-up

GDPR compliance - New standard contractual clauses

First administrative fines imposed by the Luxembourg data protection supervisory authority

European Commission's Action Plan on Intellectual Property

Luxembourg law recognises issuance of dematerialised securities in blockchains

On 21 January 2021, the Luxembourg Parliament adopted the Law of 22 January 2021 modifying the Law of 5 April 1993 on the financial sector and the Law of 6 April 2013 on dematerialised securities ("**Law of 2021**").

The Law of 2021 aims at modernising the existing legal framework for dematerialised securities, by expressly recognising the possibility to issue dematerialised securities through distributed ledger technology such as blockchains.

Please read our article **here**.

Artificial Intelligence: the Commission's Regulation Proposal and AI strategy in Luxembourg

Introduction

Artificial Intelligence ("**AI**") is developing rapidly. AI-based systems and technologies are expected to bring far-reaching social and economic benefits for individuals as well as for companies and other players in many industries such as healthcare, farming, education, energy, logistics, justice, climate change mitigation etc.[1] AI may, however, also entail a number of potential risks and generate harm to the health, safety or the fundamental rights of citizens. In light of these opportunities and associated threats, the European Commission has identified the need for a regulatory framework on AI, which is the very first of its kind.

What's new?

On 21 April 2021, the European Commission published a Proposal for a Regulation on Artificial Intelligence[2] (the "**AI Regulation Proposal**") which constitutes a decisive step in its continuous strategy for artificial intelligence aimed at putting European values at its centre.[3] In this context, as a follow-up to the Guidelines for Trustworthy AI and the White Paper on AI, the AI Regulation Proposal aims "to turn Europe into a global hub for a trustworthy AI".[4] At the same time, Luxembourg pursues its national strategy on AI by clarifying its position towards AI systems and subsequent (economic and business) opportunities.

Definition of AI systems

The AI Regulation Proposal provides first for a *future-proof*[5] definition of AI systems qualifying them as: "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[6]

Territorial and material scope

The scope of the AI Regulation Proposal is broad as it is planned to apply to:

1) Providers (whether they are public or private players) who offer and who place AI systems on the European market, irrespective of whether they are established within or outside of the European Union.

2) Users of AI systems located within the Union.

3) Providers and users of AI systems established outside the EU where the output produced by the AI system is used in the EU.

Categorisation of AI systems

The AI Regulation Proposal classifies AI systems in categories depending on the risk of potential harm they can have towards individuals and their fundamental rights. In light of this, AI systems carrying a so-called *unacceptable risk* will be prohibited, as they may constitute a *clear threat to the safety, livelihoods and rights of people.* AI systems carrying a *high risk* will be subject to a stricter regulatory regime with respect to security and accountability obligations. Finally, AI systems bearing a *limited* or *minimal risk* will have to respond to certain transparency criteria, which are all outlined in the AI Regulation Proposal.

Sanctions

In the event of non-compliance, the AI Regulation Proposal also foresees administrative fines, which can reach up to EUR 30,000,000 or 6% of the total annual turnover, whichever is higher.

Creation of a European advisory body and national supervisory authorities

A European Artificial Intelligence Board at the level of the European Union, which will be composed of representatives from all EU Member States (including Luxembourg) and the European Commission, would be established, to advise and assist the Commission in connection with the AI Regulation. At national level, Member States must designate national competent authorities and a national supervisory authority responsible for the enforcement of the regulation and to provide further guidance and advice.

Luxembourg's position and its AI strategy.

In 2019, Luxembourg launched its strategy on AI with the ambition to become one of the most advanced digital societies in the world, especially in the EU while supporting human-centric AI development.[7] In that context, on April 28, 2021, Prime Minister Xavier Bettel, also Minister of Communications and Media presented the results of a public consultation on AI.[8] For that purpose, 20,000 Luxembourg residents of the age of 16 years and over were consulted via a survey developed by Luxembourg Institute of Socio-Economic Research (LISER).

The results of the consultation showed that despite the fact that a large majority of Luxembourg citizens consider AI as a facilitator of daily life tasks (70%) and repetitive work-related tasks (64%), a certain scepticism towards AI nevertheless persists. The mistrust resides in the fact that AI may be unable to distinguish between good and bad consequences, or may eventually act in a discriminatory or biased way. However, it appears that 77% of the consulted population have solid confidence in the use of AI in the public administration, especially to reduce paperwork, but also to monitor mobility or to receive accurate medical diagnoses in the context of disease prevention.

While this public consultation gives a fair overview of how AI is currently perceived by the population, the Prime Minister emphasised the importance of an absolute respect of human rights during its development and use.

The impact of the AI Regulation Proposal

These rules will provide Europe with a leading role in setting a global standard with regard to the regulation of AI systems. In the meantime, the AI Regulation Proposal will be subject to the ordinary legislative procedure of the European Parliament. After being adopted, the AI Regulation Proposal will become a directly applicable regulation across the Member States of the European Union. Companies located outside of the European Economic Area will also have to comply with these new standards if their AI systems output affect European citizens. We will therefore remain alert on questions regarding the impact on different economic players worldwide.

As to Luxembourg, we will monitor how the government will position itself in its continuous strategy on AI, during the implementation process of the AI Regulation Proposal.

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**

This may also interest you:

- **Opinion of the EDPS on the Commission's White Paper on Artificial Intelligence**

1. Recital 3 of the AI Proposal Regulation
2. Press Release from the European Commission: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence and amending certain union legislative acts (the "Press Release") (**here**)
3. Find more information about the European Commission's Strategy **https://digital-strategy.ec.europa.eu/en/policies/strategy-artificial-intelligence**
4. Press Release
5. Press Release
6. Article 3(1) of the AI Regulation Proposal
7. Artificial Intelligence: a strategic vision for Luxembourg (**here**)
8. The entire consultation with its results is available (**here**)

The Data Governance Act – regulating access to data held by public authorities

On 25 November 2020, the European Commission published a Proposal for a Regulation on European data governance ("**Data Governance Act**"), part of a set of measures related to the **European data strategy** that aims at making the EU a leader in a

data-driven society.

This proposal addresses sharing mechanisms for data held by public sector bodies that is subject to rights of others (such as documents on which third parties hold intellectual property rights) so that legal entities may gather such data from individuals for projects of general public interest.

Please read our article **here**.

The impact of the Brexit deal on personal data transfers from the EU to the UK

On 24 December 2020, the European Union ("**EU**") and the United Kingdom ("**UK**") finally struck a deal over Brexit. They notably reached a Trade and Cooperation Agreement.

In respect of personal data protection, this Trade and Cooperation Agreement provides for a temporary period during which transfers made to the UK will not be considered as transfers within the meaning of the laws of the EU law, insofar as – inter alia – the UK Data Protection Act 2018 ("**DPA**") as amended in 2019 applies. The DPA was amended to incorporate the principles of the GDPR and has become the so-called UK GDPR. It will be applicable from 1 January 2021.

Should the UK not be granted an adequacy decision by the end of the temporary period (ending at the end of April or, if extended, June 2021), the situation will then be as if no deal intervened in this respect.

Please read our article **here**.

The European Commission recently released two draft decisions on the adequate protection of personal data by the United Kingdom.

Please read our article **here**.

GDPR - Adequacy decisions for the UK

On 28 June 2021, the European Commission adopted two adequacy decisions for the United Kingdom (the "**Adequacy Decisions**"); the first one concerning the continued free flow of personal data from the European Union (the "**EU**") to the United Kingdom (the "**UK**") under the General Data Protection Regulation 2016/679 (the "**GDPR**") and the other one under the Law Enforcement Directive.

The Adequacy Decisions come just in time to continue the bridging mechanism applicable under the Trade and Cooperation Agreement between the EU and the UK, allowing transfers of personal data from the EU to the UK for a temporary period ending on 30 June 2021.

With the adequacy decision adopted under the GDPR, the Commission confirms that the UK offers an adequate level of protection for personal data. As a consequence, the continued free flow of personal data between the EU and UK is guaranteed at least until 27 June 2025, unless extended. This adequacy decision is the first of its kind having a sunset clause.

For more information, please read our previous **article** on the topic Draft adequacy decisions for the free flow of personal data from the EU to the UK.

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**
Emmanuèle de Dampierre, Counsel **|** Tel: +352 44 66 44 5164**|** E-mail: **emmanueledampierre@elvingerhoss.lu**

This may also interest you:

- **The impact of the Brexit deal on personal data transfers from the EU to the UK**
- **Consequences of a no-deal Brexit on personal data transfers to the UK**

ePrivacy Regulation: The return?

On 10 February 2021, the Council of the European Union published a **press release** according to which the Member States' representatives at the Council (Committee of Permanent Representatives or "**Coreper**") have agreed to grant a negotiating mandate to the Council for the revised rules on the protection of privacy and confidentiality in the use of electronic communications services.

Hence, after years of a certain legislative slowdown following the publication in 2017 of the EU Commission's proposal for a regulation on the respect for private life and the protection of personal data in electronic communications ("**e-Privacy Regulation**") aiming to replace the e-Privacy Directive 2002/58/EC, such mandate of negotiation will finally permit the launch of a "trilogue" legislative process (between the Parliament, the Council and the Commission) in view to reach a final agreement on the content on the said e-Privacy Regulation (not expected any time soon though).

That said, it is interesting to note that – thanks to the GDPR itself – many businesses have already voluntarily adopted certain of the mechanisms referred to in the legislation in preparation as regards the use of cookies (cookies being one of the main blocking point of discussion). In particular, informing users about the use of cookies is now quite widespread behaviour. In contrast, dealing with consent collection is still quite inconsistent across the board.

Read more about the e-Privacy Regulation (and its interplay with GDPR) **here**.

GDPR - Transfers of personal data in the UCI world after Schrems II

Undertakings for Collective Investments ("**UCIs**") process personal data about investors who are either natural persons or legal persons represented by natural persons. Most of the time, processing operations by UCIs based in Luxembourg include transfers of personal data from Luxembourg to countries outside of the EEA. These transfers are governed by the GDPR and impacted by the so-called **"Schrems II"** ruling of 16 July 2020 from the Court of Justice of the European Union in case C-311/18. Although the ruling particularly deals with transfers to the US, it's effects are not limited to transfers to the US.

Key takeaways about the impact of Schrems II for UCIs are available **here**.

Regulating access to Open Data – free access to data held by public bodies

On 25 April 2018, as part of a package of measures aiming to facilitate the creation of a common data space in the EU, the European Commission ("**Commission**") proposed to review the Open Data Directive 2003/98/EC (as amended). Following an impact assessment carried out by the Commission, a recast of the Open Data Directive was adopted on 20 June 2019 resulting in **Directive (EU) 2019/1024 on open data and the re-use of public sector information** ("**New Open Data Directive**").

The New Open Data Directive repeals the Open Data Directive from 17 July 2021 and focuses notably on increasing business opportunities by encouraging the dissemination of dynamic data via application programming interfaces (APIs).

The Luxembourg Parliament is currently discussing a Bill of Law 7643 with a view to transposing the New Open Data Directive into Luxembourg law, which once adopted will repeal the amended Law of 4 December 2007 on the re-use of public-sector information.

Please read the article **here**.

Focus on European Commission's proposal for a Digital Services Act

On 15 December 2020, the European Commission published the Digital Services Act Package, which includes two significant proposals:

- a **proposal for a Regulation on a Single Market For Digital Services** (Digital Services Act or "**DSA**") and amending Directive 2000/31/EC ("**e-Commerce Directive**"),
- a proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act or **DMA**").

These proposals are expected to affect various types of providers of digital services (such as marketplaces, social media platforms, content-sharing platforms) in the European Union ("**EU**") and to create a safer and more open digital space while further developing the European Single Market for digital services.

The proposal for a Digital Services Act ("**DSA Proposal**") clarifies and upgrades the responsibilities and the accountability of the digital service providers with respect to any illegal content they intermediate or disseminate without wiping out past principles. The DSA Proposal sets out several layers of obligations, which shall apply to the digital service providers depending on the type of services they provide in the digital space.

For more information with respect to the DSA Proposal (context, entities targeted, key obligations, supervisory framework, sanctions), please read our article **here**.

As for the DMA, it will impose obligations for large online platforms (*e.g.* online search engines, video-sharing platform services, cloud computing services) that behave as "gatekeepers", such status being more fully defined in the DMA. The DMA aims to refrain from anti-competitive and unfair practices and ensure that gatekeepers themselves act in a way that guarantees an open online environment.

GDPR in the health research sector: EDPB response to EU Commission on a consistent application

What happened?

On 2 February 2021, the European Data Protection Board (the "**EDPB**") adopted its response to the European Commission's request for clarification on the consistent application of the GDPR[1] in the field of health research (the "**EDPB Response**")[2].

On several occasions, questions posed to the EDPB have remained partly unanswered or open. The EDPB underlines that it will soon clarify these points in its forthcoming Guidelines on the processing of personal data for scientific research purposes (to be released during 2021).

Main questions tackled by the EDPB

- **Legal basis for processing of health-related data for scientific research purposes**

A recurrent question of the European Commission (the "**EC**") concerned the appropriate legal bases to rely on for processing personal data for scientific research, especially with regard to (i) the cumulative requirements of relying on an appropriate legal basis (at least one of those listed under Article 6 of the GDPR), which may be other than consent, and on an appropriate exemption under Article 9 of the GDPR, (ii) the (in)validity of consent in the context of clinical trials (i.e. the possible imbalance of power between the data subject and the controller)[3], and (iii) the conduct of a single research project by one controller in several Member States, which may need to rely on different legal bases depending on the Member States law.

In particular, the EDPB states that the scientific ethical standards (i.e. requiring the informed consent[4] of the individuals to participate in a scientific research project) must be distinguished from the consent as a legal basis for processing personal data under Article 6(1)(a) of the GDPR and explicit consent as an exemption for processing special categories of personal data under Article 9(2)(a) of the GDPR. The ethical requirements apply in addition to the GDPR.

- **Further processing of previously collected health data**

The EDPB Response also focuses on the further processing for scientific research of previously collected health data by relying on the presumption of compatible use with the original purpose. This question is particularly important as recent experience shows that, for example, samples collected in a particular context (i.e. research in relation to a specific disease) may be of the utmost interest in another context (i.e. research related to other diseases). But for this to be of scientific interest, it is sometimes very useful to be able to contact the person from whom the sample was collected, to be able to examine contextual elements that were not initially collected. Therefore, working with samples of named individuals may become useful over time.[5] For further processing of previously collected health data in different research projects:

  - the data must be processed with adequate safeguards as required under Article 89(1) of the GDPR implemented in Luxembourg by Articles 64 and 65 of the Law of 1 August 2018[6] (e.g. appointing a data protection officer, carrying out an impact assessment, using anonymisation or pseudonymisation, using privacy enhancing technologies, logging access, adopting a code of conduct, etc.);

  - if the exemption relied on under Article 9 of the GDPR for the original purpose of the processing does not apply to the processing for scientific research purposes, the researcher must rely on a different exemption.

- **The concept of broad consent**

Another clarification concerns the so-called notion of "broad consent" used by the EC. As the concept of "broad consent" does not exist as such in the GDPR, the EDPB assumes that the EC refers to Recital 33, hence considering there is a need to clarify the meaning and scope of that Recital.

Recital 33 suggests that in some cases where the purpose of personal data processing for scientific research cannot be specified in a precise manner at the time of the collection of data, it should be possible to gather valid consent from data subjects "in more general terms and for specific stages of a research project that are already known to take place at the outset."[7] While recognising that Recital 33 allows some flexibility, the EDPB clarifies that this kind of consent has to be accompanied by adequate safeguards to enhance transparency of processing during the research project and that consent has to be specified as much and as soon as reasonably possible.

Finally, the EDPB underlines that Recital 33 should not be understood as an exception or the possibility to work around the principle to articulate in a clear manner the purpose of the processing. The purpose should always be detailed as much as possible, particularly in the initial phase of the research project.

The EDPB nevertheless says that a proper response to this question will require more analysis and discussions. The EDPB will therefore circle back in this respect in its forthcoming guidelines on the processing of personal data for scientific research purposes, expected during 2021.

- **Transparency of data processing: information to be provided to the data subject**

The transparency obligations under the GDPR require the controller to inform the data subjects about the processing of their personal data. However, the controller who has not obtained the data from the data subjects can be exempted from the information obligation as per Article 14(5)(b) of the GDPR, where it proves impossible or requires disproportionate efforts to inform data subjects of the further processing of their personal data for research purposes. This exemption does not apply where the controller collected the data directly from the data subject. Therefore, such controllers should take appropriate measures at the time of the data collection to ensure they can meet the further information requirements in the event of a further processing for research purposes.

- Anonymization, pseudonymisation and other appropriate safeguards

The EDPB pointes out that the possibility to anonymise genetic data with technical and organisational measures remains an unresolved issue. In general, the EDPB expresses its skepticism towards the possibility of anonymising genetic data. Therefore, to remain on the safe side, the EDPB advises that genetic data should be considered as if it was personal data and processed with the necessary appropriate technical and organisational measures to comply with the GDPR.

The EDPB recognises a lack of available information as to what appropriate safeguards should be considered in the context of processing for scientific research purposes. Further clarification on that matter would have to be provided.

What's next?

Although the EDPB's Response constitute a first clarification on questions arising with respect to personal data processed in the context of national and transnational scientific research projects, controllers and researchers must remain faithful to the upcoming EDPB Guidelines on the processing of personal data for scientific research purposes, expected to clarify remaining uncertainties.

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**

This may also interest you:

- **EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak**
- **The use of mobile applications in the fight against COVID-19 – Guidelines from the EDPB**
- **COVID 19 - Legal principles and CNPD best practices in relation to processing by employers of health data**

1. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data.
2. **EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research**
3. By reference to the **EDPB Opinion 3/2019**

4. In addition, Article 28.1(b) and (c) of **Regulation (EU) No 536/2014 of 16 April 2014 on clinical trials on medicinal products for human use** provides that "a clinical trial may be conducted only where (...) the subjects, or where a subject is not able to give informed consent, his or her legally designated representative, have been informed in accordance with Article 29(2) to (6) [and] given informed consent in accordance with Article 29(1), (7) and (8)." The timing of the application of this Regulation in all Member States depends on when the so-called EU clinical trials information system will be fully functional (planned to go live in 2022).
5. See below about the EDPB scepticism on the possibility to anonymise genetic data.
6. Law of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.
7. Point 26 of the EDPB Response.

Guidelines regarding the geolocation of vehicles made available to employees

On 15 April 2021, the *Commission Nationale pour la Protection des Données* ("**CNPD**"), the Luxembourg Data Protection Authority, published new guidelines on the geolocation of company vehicles made available to employees (the "**Guidelines**").

The use of company vehicles and their subsequent geolocation involves the processing of personal data. Therefore, the CNPD raises certain data protection questions and risks for the privacy of employees and states again that the geolocation of vehicles made available to employees has always to be considered as processing of personal data for surveillance purposes within the meaning of Article L. 261-1 of the Luxembourg Labour Code.

In the Guidelines, the CNPD reiterates some of the main principles and obligations applicable to the geolocation of employees with regard to the existing legislation on the protection of personal data.[1]

The entire Guidelines are available on the website of the CNPD at **https://cnpd.public.lu/fr/dossiers-thematiques/geolocalisation-vehicules.html**.

For more information on the process to be followed before implementing surveillance measures at the workplace such as video-surveillance, telephone recordings, geolocation, etc. please contact our ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**

This may also interest you:

- **New law on monitoring at the workplace**

1. Including the General Data Protection Regulation

Digital Green Pass: EU data protection authorities' position

What happened?

On 31 March 2021, the European Data Protection Board (the **EDPB**) and the European Data Protection Supervisor (the **EDPS**, together the **Authorities**) adopted a **joint opinion** on the European Commission's proposal to create a **Digital Green Certificate** (the **Proposal**), also known as the Digital Green Pass.

The objective of the Digital Green Certificate is to allow individuals vaccinated against COVID-19 to move freely within the EEA during the ongoing pandemic. The Proposal aims at setting out a common framework for the implementation of a Digital Green Certificate, allowing interoperability between the different measures and solutions implemented across EU Member States.

What is the main takeaway?

The Authorities do not consider the protection of personal data as an obstacle for fighting the COVID-19 pandemic but says the Digital Green Certificate should fully comply with European legislation on data protection such as the **General Data Protection Regulation** (the **GDPR**).

What are the main concerns of the Authorities?

The Authorities say that:

- the Proposal lacks an impact assessment and should fairly balance the objectives of general interest pursued by the Digital Green Certificate and the respect of fundamental rights such as the right to privacy and the protection of personal data;
- the Digital Green Certificate should not be understood as proof of a time-stamped factual medical application or history facilitating free movement within the EEA; it must not be intended as an immunity or non-contagiousness certificate;
- they are concerned about any potential further use of data collected once the current COVID-19 pandemic has ended, yet suggesting that the Regulation to be adopted should expressly prohibit any such subsequent use and, therefore, the words "or similar infectious diseases with epidemic potential" should be deleted from the current wording when referring to COVID-19;
- while this is not a purpose stated in the Proposal, it is likely that EU Member States will use the Digital Green Certificate for domestic purposes, such as controlling access to pubs and shops; EU Member States will have to take into account Article 6(4) of the GDPR and therefore provide for a comprehensive legal basis for any use of the Digital Green Certificate for purposes other than that for which the personal data have been initially collected (i.e. facilitating free movement within the EEA);
- the Digital Green Certificate should better define its purpose and provide for a mechanism for monitoring its use, be of a temporary nature and provide for security measures (notably to mitigate the risk linked to forgery as is the case with false COVID-19 test certificates that exist);
- the Proposal does not allow for the creation of any sort of personal data central database at EU level, and must not lead to any such creation under the pretext of the establishment of the Digital Green Certificate framework.

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**

This may also interest you:

- GDPR in the health research sector: EDPB response to EU Commission on a consistent application
- EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- The use of mobile applications in the fight against COVID-19 – Guidelines from the EDPB
- COVID 19 - Legal principles and CNPD best practices in relation to processing by employers of health data

GDPR anniversary - Time to take your business for a data protection compliance check-up

It's already the third anniversary of the GDPR!

Here are 10 questions that controllers should consider when self-assessing their compliance. Most of these questions are relevant for processors too!

1. Have you set up and maintained a record/register of processing activities?

2. Are you identifying, on an ongoing basis, lawful bases for all the processing you carry out (including recording consent as appropriate and conducting a balancing test if relying on legitimate interest)?

3. Are you drafting or updating your internal data protection policy and privacy information notice?

4. Are you putting in place processes and procedures to respond to data subjects' requests (access, update, erasure, etc.) and managing data breaches?

5. Destroying or deleting personal data that is no longer necessary to pursue the purposes for which it has been collected?

6. Implementing appropriate technical and organisational measures to protect personal data (including an information security policy and training for the member of your staff who processes personal data) and are you regularly reviewing the security of your IT environment?

7. Have you entered into a written contract with the processors you use?

8. Do you have documents that you do not need and have you conducted data protection impact assessments (DPIA)?

9. Have you appointed a DPO?

10. Are you ensuring all transfers of personal data are made under appropriate safeguards and are you taking appropriate measures further to the Schrems II case?

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**

GDPR compliance – New standard contractual clauses

On 4 June 2021, the European Commission adopted the following two sets of new standard contractual clauses in the context of the General Data Protection Regulation (Regulation 2016/679, the **GDPR**):

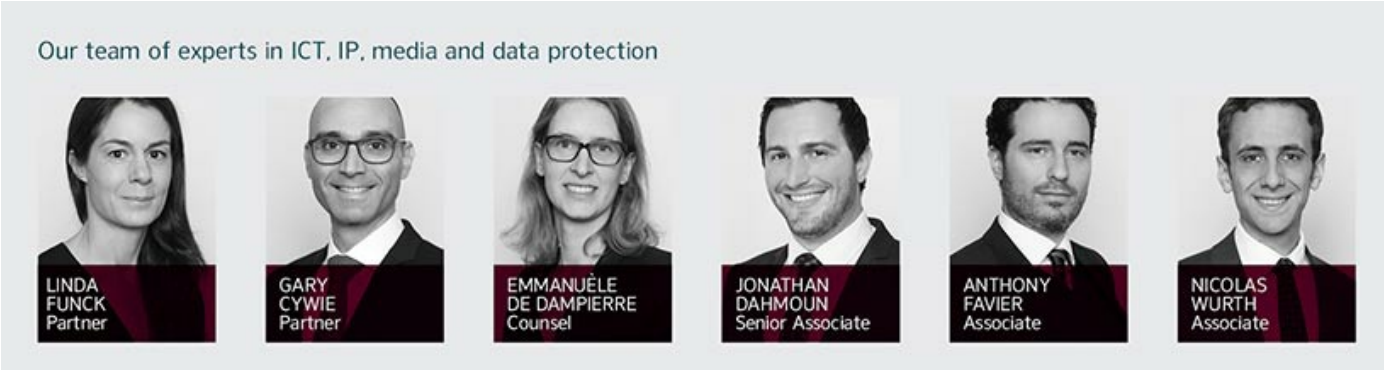
- standard contractual clauses replacing the old standard contractual clauses providing appropriate safeguards within the meaning of Article 46(1) and (2)(c) of the GDPR for the transfer of personal data by a controller or processor (data exporter) to a controller or (sub-)processor whose processing is not subject to the GDPR (data importer);[1] and
- standard contractual clauses that can be used in contracts between controllers and processors who process personal data on behalf of the controller(s) for compliance with the requirements of Article 28(3) and (4) of the GDPR, regardless of whether there is a transfer or not;[2]

The main innovation in the standard contractual clauses for transfers of personal data to third countries reside in its modular structure giving the flexibility to cover various transfer scenarios within one single document, i.e. transfers from controller to controller, from controller to processor; from processor to processor and from processor to controller. The same set of standard contractual clauses equally covers the rights and obligations of controllers and processors with respect to the requirements in Article 28(3) and (4) of the GDPR.

These standard contractual clauses for transfers notably reflect some requirements deriving from the GDPR as interpreted in the light of the relatively recent developments on international transfers of personal data further to the outcome of the "Schrems II" case. Nevertheless, they do not remove the consequences of the CJEU ruling and the need to assess the necessity to adopt supplemental measures as recommended by the European Data Protection Board (in a version adopted for public consultations). On the foregoing and the consequences of Schrems II in particular, please see our **article**.

The decisions adopting the standard contractual clauses will enter into force on 27 June 2021.

Former standard contractual clauses will be repealed on 27 September 2021. Contracts concluded before that day that rely on former standard contractual clauses will remain valid for a period of 15 months ending on 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of the GDPR.



Find out more about our ICT, IP, media and data protection practice area.

1. See **Commission Implementing Decision 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation 2016/679 and Article 29(7) of Regulation 2018/1725**.
2. See **Commission Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation 2016/679**.

First administrative fines imposed by the Luxembourg data protection supervisory authority

On 7 June 2021, the Luxembourg National Data Protection Commission (*Commission Nationale pour la Protection des Données* – the "**CNPD**") published 18 decisions:

- in nine decisions, the CNPD found that controllers (Luxembourg-based companies) did not breach any of the provisions of the (EU) General Data Protection Regulation 2016/679 (the "**GDPR**") and decided therefore to close the ongoing investigation;
- in six decisions, the CNPD issued a formal warning *(rappel à l'ordre)* or an injunction to comply *(injonction de se mettre en conformité)* to companies due to breaches of the GDPR (sometimes associated with a fine);
- finally, in six cases, the CNPD decided to impose administrative fines on the entities concerned due to more significant violations of the GDPR.

This is the very first set of administrative fines the CNPD has issued since the entry into force of the GDPR. These 18 decisions are the result of enquiries and audits led by the CNPD towards several companies that were selected according to various criteria such as:

- the size of the organisations,
- the sensitivity of the data processed and the associated risk for the data subject, and
- the sector of activity (e.g. the insurance sector)[1].

The CNPD noted that the entities subject to administrative fines either failed to comply with key principles of the GDPR, such as the principle of data minimisation, the principle of transparency or did not adequately put in place appropriate security measures or did not appoint a Data Protection Officer ("**DPO**") as is required by the GDPR under certain criteria. As a consequence of these breaches, the CNPD imposed administrative fines ranging from EUR 1,000 to EUR 18,000.

In one of the decisions, the CNPD reminded the importance of the DPO's involvement at the earliest possible stage in all data protection issues and the need to have necessary resources and time to carry out his/her data protection duties.

A decision rendered by the CNPD may be appealed before the administrative court within three months following its notification to the entity concerned.

All the decisions published by the CNPD can be consulted **here**. Please note that these decisions are anonymised.

For any questions please contact the ICT, IP, media and data protection team:

Linda Funck, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **|** Tel: +352 44 66 44 5164**|** E-mail: **garycywie@elvingerhoss.lu**
Emmanuèle de Dampierre, Counsel **|** Tel: +352 44 66 44 5164**|** E-mail: **emmanueledampierre@elvingerhoss.lu**

1. National Data Protection Commission (*Commission Nationale pour la Protection des Données)* – Annual report p. 43

European Commission's Action Plan on Intellectual Property

On 25 November 2020, the European Commission ("**Commission**") published its Action Plan on Intellectual Property[1] ("**Action Plan**") which proposes to implement specific intellectual property ("**IP**") policies with the particular objective of modernising the European Union ("**EU**") framework in this field and helping small and medium enterprises ("**SMEs**") benefit from their inventions and creations, especially in times of health and economic crisis.

This Action Plan is an ambitious policy document with multiple proposals for actions ("democratising" IP, enhanced support to SMEs, fight against infringements of IP rights, etc.). It also highlights several developments that are expected with regard to patents, author's rights, databases, trade secrets or designs in the following months/years.

Please click **here** to read our article.

1. **Communication** from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: "Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience".