TABLE OF CONTENTS

EACCNY "Brexit, What's Next?" Series | EU-UK Data Protection Law Divergence: Impact on Data flows

*First published on **www.eacny.com***

1. Post-Brexit UK regime

Following the end of the Brexit transition period, the United Kingdom has retained the General Data Protection Regulation (**Regulation 2016/679**) ("**EU GDPR**") as part of its national laws, as the "**UK GDPR**", under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (as amended) ("**Regulations**").

The UK GDPR sits alongside the Data Protection Act 2018 ("**DPA**") and the Privacy and Electronic Communications Regulations ("**PECR**") as the backbone of the UK's post-Brexit data protection regime. The Regulations amended the UK GDPR, DPA and PECR to make them work properly as domestic law through relatively functional changes, under which the key substance of the EU GDPR remained. However, the UK now could diverge from EU data protection law through domestic statutory reform and the UK Government is considering steps in that direction.

2. Adequacy Decisions adopted

On 28 June 2021, just before the interim bridging mechanism enshrined in the EU-UK Trade and Cooperation Agreement expired on 30 June 2021, the European Commission ("**Commission**") adopted two adequacy decisions for the UK ("**Adequacy Decisions**"). The first decision concerned the EU **GDPR** and the second Law Enforcement Directive.

The adoption of the Adequacy Decisions, after months of negotiation, provided a degree of long-awaited legal certainty

concerning the ongoing flow of personal data from the EU to the UK, including data exchanges in the law enforcement sector. Under this regime, businesses located in the EU can continue exporting personal data to the UK as current UK national laws have been recognised as offering a level of protection that is essentially equivalent to that under the EU GDPR.

The Adequacy Decisions are the first of their kind to have a sunset clause limiting their duration. The Adequacy Decisions expire four years from their entry into force, after which they can be further extended. This sunset clause has been introduced to ensure that UK data protection law remains essentially equivalent to that of the EU while the UK is covered by adequacy decisions. This is a strong safeguard in case there is future divergence in UK data protection law away from the essentially equivalent level of protection which existed at the time of the assessment.

UK Consultation on Data Protection Reform

On 10 September 2021, the UK's Department for Digital, Culture, Media & Sport ("**DCMS**") released a consultation "**Data: A new direction**" (the "**Consultation**") with suggested reforms to the UK's data protection regime. The aim of the Consultation is to "create an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data". The Consultation's proposals represent significant divergence from the EU regime and trend towards a risk-based approach.

The key points are:

- **Accountability and governance.** Revoking existing obligations to perform data protection impact assessments, maintain records of processing, and appoint a data protection officer. These would be replaced by a privacy management program ("**PMP**"), which is intended to be a less rigid approach to accountability although the substance is relatively similar to the UK GDPR requirements. The proposed PMP demands clear responsibilities for compliance, policies and risk assessment tools and operational plans to monitor and revise the PMP.
- **Adequacy decisions.** Amending the framework for the UK's own adequacy decisions for data transfers, to be *"risk-based and focused on outcomes"* rather than a "*largely textual comparison of another country's legislation"* focussing on *"academic or immaterial"* risks. Adequacy decisions may also be included as a part of trade agreements with other countries. We observe the announcement from the DCMS that "*adequacy partnerships*" are already being progressed with many jurisdictions, including the US. That would represent a significant change from the EU approach, as the Commission is currently talking down prospects for an imminent replacement for the (now invalid) Privacy Shield transfer mechanism.
- **International Transfers.** Allowing organisations to create alternative transfer mechanisms, in addition to the standard form mechanisms already available under Article 46 of the UK GDPR. This may even look like a move back to the UK's pre-EU GDPR approach of allowing exporters to draft their own contractual transfer safeguards. This could benefit organisations with complex data transfer requirements for which the existing suite of mechanisms, such as the Standard Contractual Clauses, are not an effective way of safeguarding a data transfer.
- **Data breach reporting.** Stating that only data breaches that are likely to create a risk to the rights and freedoms of individuals **and** which are material would need to be reported to the Information Commissioner's Office ("**ICO**"). This would create different standards for reporting under the UK GDPR compared with the EU requirement, causing more complexities for organisations with a multi-national footprint.
- **DSAR's.** Reintroducing a nominal fee from the data subject for a data subject access request ("**DSAR**") along with the ability to impose a cost ceiling on a DSAR response and to refuse vexatious requests.
- **Legitimate interests.** Publishing a list of pre-approved legitimate interests, on which an organisation could rely without the need to balance that interest against an individual's rights. Notably, the list includes audience measurement cookies for service users' devices, and the use of personal data for research and development to improve services.

Impact of Reform on Adequacy Decisions

On 13 April 2021, the EDPB adopted Opinion 14/2021 regarding the Commission's (then) draft adequacy decision of the UK under the EU GDPR.[1] At the time of providing that Opinion, the UK data protection framework was largely based on the EU data protection framework because the UK was a Member State of the EU up until 31 January 2020.

The EDPB nevertheless raised serious challenges and concerns to be monitored by the UK and the Commission, in particular: national security; intelligence and the surveillance regime of the UK (including access by public authorities to data transferred to the UK); and possible future divergence of the UK data protection framework. The resulting Adequacy Decisions follow a careful assessment by the Commission of UK law and practice with those challenges in mind. The conclusion of that assessment resides notably in the application of the DPA as amended to incorporate the principles of the EU GDPR into the UK GDPR, adhesion to the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (and Protocol 108+) and submission to the European Court of Human Rights.

Therefore, any amendment to the legal framework currently applicable in the UK and affecting its essentially equivalent level of

data protection could put the Adequacy Decisions at risk. The Commission shall indeed, according to the Adequacy Decisions themselves, "*continuously monitor the application of the UK legal framework upon which the Adequacy Decisions are based, including the conditions under which onward transfers are carried out and individual rights are exercised*". In addition, EU "*Member States and the European Commission shall inform each other of [(a)] cases where the Information Commissioner, or any other competent United Kingdom authority, fails to ensure compliance with the legal framework upon which [the Adequacy Decisions are] based"* and of "*[(b)] any indications that interferences by United Kingdom public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences*".

Should the Commission become aware of indications that an adequate level of protection is no longer ensured, it can suspend, repeal or amend the Adequacy Decisions after informing the competent UK authorities. The Commission can also do the same in the event that adequacy can no longer be assessed due to any lack of cooperation of UK Government.

3. Key Questions for International Companies Present in the UK and EU

One-stop-shop and double jeopardy

Under the EU GDPR, an organisation engaged in cross-border processing may use the supervisory authority in the EU Member State where it has its main establishment as its lead supervisory authority ("**LSA**"). The benefit of this is that the LSA will be the sole interlocutor, or one-stop-shop ("**OSS**"), for that organisation. That mechanism no longer applies to the UK following the end of the Brexit transition period.

The UK GDPR applies to the processing of personal data by: (a) UK-established businesses; and (b) controllers and processors established outside of the UK if their processing activities relate to offering goods or services to individuals in the UK or monitoring the behaviour of individuals taking place in the UK.

The EU GDPR in turn applies to the processing of personal data by: (a) EU-established businesses; and (b) controllers and processors established outside of the EU but offering goods or services to individuals in the EU or monitoring the behaviour of individuals taking place in the EU.

As a result, the two regimes may apply concurrently to the same processing activities by either UK-based businesses active in the EU or EU-based businesses active in the UK. Therefore, both UK-based and EU-based controllers and processors may fall within the scope of the supervision of the ICO and one or several supervisory authorities in the European Economic Area ("**EEA**"), with or without application of the OSS mechanisms. They may even face the "double jeopardy" of fines or other enforcement action being taken under both the EU GDPR and the UK GDPR. This will depend on whether or not any processing can be considered as cross-border and whether or not it is likely to substantially affect individuals in EEA states other than the one where the controller or processor is established.

One transfer, two regimes

A similar conclusion applies to transfers from the UK or the EEA to countries outside of the EEA as these transfers might fall within the scope of the UK GDPR (regarding personal data collected in the UK or otherwise subject to the UK GDPR) and of the EU GDPR (regarding personal data collected in the EEA or otherwise subject to the EU GDPR). Other than that, transfers to the EEA are currently made under the relevant adequacy decision and transfers from the UK to the EEA do not require any specific safeguard by virtue of the Adequacy Decisions.

UK and EU Representatives

The Adequacy Decisions do not relieve UK-based controllers and processors from appointing an EU representative as is required under Article 27 EU GDPR if and to the extent that the EU GDPR applies to them.

One often-neglected consequence of the move to the UK GDPR is that a UK representative must now be appointed by a non-UK-based data controller or processor where it is subject to the UK GDPR. That requirement applies if the processing by a data controller or processor relates to the offering of goods and services to, or monitoring of, data subjects in the UK and the organisation is not established in the UK. There are exceptions from that requirement for occasional and small scale or non-special category processing which mirror that under the EU GDPR itself. The ICO is yet to publish any enforcement action it has taken in relation to the failure to appoint a UK representative.

4. International Transfers

Chapter V of the UK GDPR requires there to be appropriate safeguards for international transfers of data to outside of the UK. To the extent that a UK GDPR adequacy decision is unavailable, alternative safeguards are provided for under Article 46 of the UK GDPR. In addition, as the *Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems* (Case C-311/18) ("**Schrems II** case was decided prior to the end of the Brexit transition period, it still applies as retained EU law, from which only the UK's higher courts may diverge. This means that exporters must ensure that data receives "substantially similar" protections in

the country importing the data to those available under the UK GDPR, including that enforceable data subject rights and remedies are available.

The ICO has proposed UK-specific transfer safeguards to fulfil the requirements of Article 46 of the UK GDPR. In particular, it has published a draft international data transfer agreement ("**IDTA**") (effectively a UK version of the EU's Standard Contractual Clauses ("**EU SCCs**")), for use when exporting personal data to a third country. There are distinct differences between the IDTA and the EU SCCs, from the "plain English" drafting of the IDTA down to the different types of transfer that each may cover.

Organisations subject to both the EU and the UK GDPR may wonder whether they will need to put in place two transfer safeguards for the same transfer. This is not necessarily the case, as the ICO has also published a draft short form "UK Addendum". This is intended to be used alongside the EU SCCs as an approved safeguard under the UK GDPR, in place of the IDTA. The UK Addendum makes minor amendments to the EU SCCs, to make them work in the context of the UK GDPR. The UK Addendum is likely to be commercially preferable to organisations that have already updated their EU SCCs within their data transfer agreements, because simply adding the UK Addendum will facilitate compliance with the UK GDPR without the full IDTA.

Alongside the IDTA, the ICO published a draft transfer risk assessment ("**TRA**"), which is designed to be used to fulfil the *Schrems II* requirement to assess transfer risks and to ensure equivalent protection is available before making a third country transfer. Again, the TRA takes a relatively different, arguably more pragmatic, approach to risk assessment, at least compared to the EDPB guidance on the topic.

UK to EU Transfers

At present, transfers from the UK to the EU are safeguarded by the Adequacy Decisions, adopted on 28 June 2021. To the extent that the Consultation proposes significant divergences by the UK from the EU GDPR, this may impact these Adequacy Decisions. This would of course introduce significant friction for EEA-UK data flows.

Updates to the EU SCCs and remediation

The Commission adopted the following two sets of EU SCCs in the context of the EU GDPR, that entered into force on 27 June 2021:

- EU SCCs replacing the old standard contractual clauses ("**Old EU SCCs**") providing appropriate safeguards within the meaning of Article 46(1) and (2)(c) of the EU 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 EU GDPR (data importer); and
- EU SCCs that can be used in contracts between controllers and processors that 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.

The main innovation in the EU SCCs 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 EU SCCs equally cover the rights and obligations of controllers and processors with respect to the requirements in Article 28(3) and (4) of the EU GDPR.

These EU SCCs for transfers notably reflect some requirements deriving from the EU GDPR as interpreted in the light of the outcome of Schrems II. 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 EDPB (in a version adopted for public consultation).

The Old EU SCCs were repealed on 27 September 2021. Contracts concluded before that day that rely on the Old EU SCCs will remain valid until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on the Old EU SCCs ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of the EU GDPR.

5. Future Developments

UK's Approach to the ePrivacy Regulation

The ePrivacy Regulation, once finalised and implemented, will be EU law and thus not directly applicable as part of the UK data protection regime. However, the developments will be relevant for many UK companies that are likely to fall within its extra-territorial scope.

This may raise complex issues, as the UK Consultation also proposes amendments to PECR, which may conflict with the changes that are proposed in the current draft of the ePrivacy Regulation. For example, the Consultation proposes removing the requirement to obtain consent for analytics cookies and permitting websites to use "legitimate interest" cookies without obtaining

consent for limited purposes.

It is also possible that the UK will not follow the EU's lead on the many other planned legislative developments, such as the proposed EU Regulation on Data Governance.

Organisations will therefore need to navigate a patchwork of data-related obligations that will apply across the UK and EU.

Authors:
Gary Cywie, *Partner*
ELVINGER HOSS PRUSSEN | **garycywie@elvingerhoss.lu**
Katie Hewson, *Partner*
STEPHENSON HARWOOD | **katie.hewson@shlegal.com**
Jonathan Howie, *Trainee Solicitor*
STEPHENSON HARWOOD | **jonathan.howie@shlegal.com**

1. Opinion 14/2021 regarding the Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, pt. 37 (available at **https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf**).

EU adequacy decision for South Korea

On 17 December 2021, the European Commission ("**Commission**") adopted an adequacy decision for the Republic of Korea.[1] This adequacy decision allows the free flow of personal data from the EU to Korea, without any further need for additional safeguards.[2]

The Commission will conduct a first review of the decision after three years to evaluate the functioning of this framework. After this initial review, periodic reviews of this framework will take place at least every four years.

For more information on the adequacy decision, please consult its related **FAQ**.

A fully updated list of the countries benefiting from an adequate level of data protection can be consulted on the Commission's dedicated **webpage**.

1. Commission implementing decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act.
2. Such as standard contractual clauses.

European Electronic Communication Code adopted

What happened?

The **Law of 17 December 2021 on electronic communications networks and services** ("**Law**") was published on 22 December 2021 and came into force on 26 December 2021. It repeals the former regime set out by the Law of 27 February 2011 on electronic communications networks and services.

What is the main takeaway?

The new legislative regime transposes into Luxembourg law the **European Electronic Communications Code** ("**EECC**") established by Directive (EU) 2018/1972.

The EECC forms part of a package of telecom laws and aims at updating the rules governing the telecoms sector. It regulates electronic communications networks and services with new or revised rules and sets out tasks for national regulatory authorities, in Luxembourg the *Institut Luxembourgeois de Regulation* ("**ILR**"). The ILR is a member of the Body of European Regulators for

Electronic Communications ("**BEREC**") set up by one of the laws of the EU telecom package. The Law also integrates certain national provisions not originating from the EECC but from the Law of 21 March 1997 on telecommunications (pushed since then into the Law of 30 May 2005 on electronic communication networks and services).

What are the main changes?

The general objectives of the EECC are to promote connectivity through and access to high capacity networks (such as 5G networks), effective competition, the security of networks and services and addresses the needs of certain social groups, in particular people with disabilities. The EECC aims at taking into account today's reality of the provision of digital services: the convergence of telecommunications, media and information technology.

In order to follow these general political objectives, the EECC notably requires that local regulation and regulators (i) provide operators with predictable regulation, (ii) ensure there is no discrimination between network and service providers operating under similar circumstances, and (iii) apply the regulation in a technology neutral fashion whenever possible and relevant.

Consequently, the scope of the Law, regulating the electronic communications, now also extends to many over-the-top players ("**OTT**"), i.e. personal communication services not subject to numbering resources such as messaging apps (including instant messaging, electronic mail and video conferencing), streaming services and connected devices. Both types of services are now subject to *ex ante* supervision. Security requirements for OTT services should, however, be adapted as they are considered in general as presenting lower risks than traditional electronic communication services as they do not control the effective convey signals over networks (with some exceptions).

Consumer protection is reinforced (information to be provided prior to the conclusion of a contract for communication services, possibility to compare offers, tariffs and quality of services, possibility to monitor the level of consumption of services included in a subscription) and the universal service now incorporates adequate and affordable access to broadband Internet.

In terms of security, the Law provides for the possibility of taking certain measures (including prohibition) for the use in public networks of equipment or software which are the source of a serious threat to the security of networks and services and having an impact on national security. This aims in particular at remedying threats related to the intrusion or interference from private or public third-party players on electronic communications networks and services, an outside control over them, or even espionage situations. This task is entrusted to the Government Council on proposal from the relevant ministry, with the assistance as appropriate of the National Committee of Communications. Nevertheless, it remains the operators' own responsibility to ensure the security of their networks.

Content is not regulated under the EECC, which focuses on electronic communications networks and services.

What's next?

Operators of telecommunication networks and related services are generally already well informed of the applicable regime. OTT service providers, however, are not necessarily familiar with electronic communication services regulation and need to understand how their own services may be affected and how to comply with the regulatory changes.

Updated CNPD's FAQ on CovidCheck controls

Following the latest legislative developments in the Grand-Duchy of Luxembourg based on the adoption of the Law dated 16 December 2021, amending the Law of 17 July 2020 on measures to combat Covid-19 ("**Covid Law**"), on 12 January 2022 the national data protection supervisory authority (*Commission Nationale pour la Protection des Données*, "**CNPD**") updated its FAQ on data protection and CovidCheck.

The updated **FAQ** (only available in French for the moment) notably details the strict conditions under which employers are authorised to set up a list of vaccinated or recovered employees to facilitate checks on the validity of their certificates. In particular, registration on a list must be voluntary meaning that employees must give their explicit consent (also meaning that they can request deletion from the list at any time without justification), the list can only contain limited information aimed at verifying the controls pertaining to the CovidCheck and is limited in time.

Please see our other **publication** for more information about the mandatory CovidCheck controls in the workspace based on the Covid Law.

Consumer Code modernised to cover digital goods and services

What happened?

The new Law of 8 December 2021 transposes and integrates into the Luxembourg Consumer Code the requirements set out under the Directive (EU) 2019/770 dedicated to the supply of digital content and services ("**DCD**") and the Directive (EU) 2019/771 governing the sale of goods ("**SGD**").

What's the main takeaway?

This new legal framework modernises the legal guarantee of conformity for the sale of goods and introduces a new regime in terms of the legal guarantee of conformity for digital content and services. Indeed, in the case of goods comprising digital elements, when the contract provides for the continuous supply of the digital content or digital service for a certain period, the seller is now liable for any lack of conformity of the digital content or service that occurs or appears within two years from the time where the said goods with the digital elements have been delivered.

For more information about the DCD and the SGD, please read **here**.

What's next?

The Luxembourg Consumer Code should soon be modified again, subject to the adoption of Bill of law 7904 currently being debated in the Parliament. That Bill of law aims at transposing the "Omnibus" Directive (UE) 2019/2161, mostly dealing with consumer law in relation to price indication and sanctions.

Artificial Intelligence in Financial Services in Europe

Elvinger Hoss and Prussen contributed the Luxembourg section of this EU multi-jurisdictional brochure prepared under the direction of Covington.

It outlines the context of the regulation of AI in the Luxembourg financial sector and summarises the rules that are currently applicable.

For any questions, please contact:

Gary Cywie, Partner **garycywie@elvingerhoss.lu**
Thomas Göricke, Counsel **thomasgoericke@elvingerhoss.lu**
Anaïs Sohler, Senior Associate **anaissohler@elvingerhoss.lu**

A refresh of certain trademark rules thanks to AC Milan

What happened?

In February 2017, the well-known football club Associazione Calcio Milan SpA ("AC Milan") filed an application to register its emblem as an international trademark designating the EU for many goods including goods in Class 16 (paper, cardboard, stationery items, writing materials, etc.).

Defending its German word trademark "Milan" registered in 1988 for goods such as "paper", "cardboards", "stationery" in Class 16, the German office supply store InterES[1] introduced an opposition before the European Union Intellectual Property Office (EUIPO) to prevent the registration of AC Milan's trademark application with respect to the goods mentioned above. InterES was claiming the existence of a risk of confusion between its prior trademark and AC Milan's trademark application for these goods.

The signs at issue were the following:

AC MILAN	Milan
Trademark application	Earlier trademark

Both the EUIPO's Opposition Division and the Board of Appeal upheld the opposition, which led AC Milan to request the annulment of the Board of Appeal's decision before the General Court of the European Union (the "General Court"). On 10 November 2021, the General Court dismissed AC Milan's action in its entirety[2].

What is the key takeaway?

Quite classical, this judgment is an opportunity to refresh some key rules of trademark law.

- Clarifications regarding the genuine use of the earlier trademark

Facing a common challenge when filing an opposition, InterES was asked to prove the genuine use of its earlier trademark.

The General Court restates that the purpose of this rule is to ensure that the earlier trademark is used in accordance with its prime function of guaranteeing the identity of the origin of the goods or services for which it is registered. The symbolic use of a trademark only to maintain artificially the rights over a trademark is not acceptable.

The evidence brought by the opponent regarding the genuine use of its trademark must be assessed as a whole and not independently from each other. Consequently, information present in certain documents (such as invoices, catalogues) can corroborate information included in other evidence (such as an affidavit regarding sales figures) even if some documents do not refer to the relevant period to be taken into consideration to assess the genuine nature of the use.

Moreover, although the earlier sign registered was a word trademark, InterES also provided proof of use in connection with the sign reproduced below:

The evidence provided was not rejected and this was the occasion for the General Court to reaffirm that the use of a sign that is not identical to the one registered is admitted. Modifications to adapt to the constraints or evolutions of one's business are allowed to the extent that these modifications do not alter the distinctive character of the registered trademark.

In the case at hand, the General Court considered that the differences between the earlier registered trademark and the sign also used in the market by InterES (addition of a figurative element, slight styling of the word element and sign represented in blue), although not negligible, do not have an impact on the distinctive character of the earlier trademark Milan.

- Importance of the principle of interdependence in the assessment of the risk of confusion

When the signs or the goods or services at stake are not identical but only similar, an opposition will be considered as well-founded if there exists a risk of confusion on the part of the public in the territory in which the earlier trademark is protected, i.e. Germany in the case at hand. A risk of confusion exists if the relevant public might believe that the goods or services marketed under the earlier trademark and the sign for which a trademark application has been filed come from the same company (or related ones). It is settled case law that the risk of confusion must be assessed globally, taking into consideration all the relevant

factors in the case.

In this respect, the principle of interdependence of the relevant factors entails considering that a low degree of similarity between the designated goods or services may be compensated by a high degree of similarity between the earlier trademark and the sign for which registration is sought, and *vice versa*[3].

In light of this principle, the risk of confusion was confirmed in the case at hand. The General Court considered that the element "AC MILAN" constituted the dominant element of the sign reproduced in the trademark application and that the visual differences existing between the signs at stake were offset by the high degree of similarity of the concerned goods i.e. stationery items and writing materials.

Further points of attention: the role of the respective reputation of the conflicting signs when assessing the risk of confusion

The Milanese football club was arguing that the Board of Appeal should have taken into account, in the context of the assessment of the risk of confusion, the high reputation of the sign applied for and of the club AC Milan.

The General Court dismissed the argument in a terse way and reaffirmed that only the reputation of the earlier trademark shall be taken into account in order to assess whether the similarity of the goods designated by the conflicting signs is sufficient to lead to a risk of confusion. This rule tends to protect the owners of existing trademarks against subsequent trademark applications for signs already known to the general public.

In the past, however, the position of the Court of Justice of the European Union (the "Court") has not always been as clear-cut. In a recent decision concerning opposition proceedings involving another player in the world of football, the Argentine footballer Lionel Messi who, in 2011, had filed the trademark application

(in particular for clothing and sporting goods), the Court did take into account the reputation of the owner of the trademark application.

In its decision of 17 September 2020[4], the Court considered it was necessary to take into account all the relevant factors in the overall assessment of the risk of confusion and in particular the reputation of the person requesting one's name to be registered as a trademark, since this reputation may have an influence on the perception of the trademark by the relevant public.

In application of this principle, the Court confirmed that Mr. Messi's reputation was leading to a difference from a conceptual point of view between the word elements "Messi" and "Massi" (the earlier European Union trademark on which the opposition was based) thus preventing any risk of confusion between the conflicting signs. One may wonder whether the decision would have been the same if Mr. Messi had not filed the above-mentioned trademark application directly, but through a company, for instance.

Given the importance of the reputation criterion in the assessment of the risk of confusion, a clarification on the role of this criterion would be welcome to increase legal certainty for trademark applicants in their trademark filing strategy and for opponents in their defence strategy.

For any questions, please contact:

Linda Funck, Partner **lindafunck@elvingerhoss.lu**
Gary Cywie, Partner **garycywie@elvingerhoss.lu**
Emmanuèle de Dampierre, Counsel **emmanuelededampierre@elvingerhoss.lu**

1. The full company name is InterES Handels- und Dienstleistungs Gesellschaft mbH & Co. KG.
2. **Judgment of the General Court (Sixth Chamber) of 10 November 2021, Associazione Calcio Milan SpA (AC Milan) v European Union Intellectual Property Office, T-353/20.**
3. See for instance Judgment of the Court of Justice of 29 September 1998, Canon Kabushiki Kaisha v Metro-Goldwyn-Mayer Inc. (C-39/97), §17.

4. Judgment of the Court of Justice of 17 September 2020, EUIPO v Lionel Andrés Messi Cuccittini and J.M.-E.V. e hijos SRL, C-449/18 and C-474/18.

The CSSF publishes a White Paper on Distributed Ledger Technologies (DLT) and blockchain

On 21 January 2022, the Luxembourg Financial Authority (the "*Commission de Surveillance du Secteur Financier*" or "**CSSF**") provided guidance with regard to the use of the DLT in the financial sector by publishing a ***Communiqué*** together with a **press release** and a **white paper** (the "**White Paper**").

Context of publication of the White Paper

In the presence of constantly evolving technologies, it is important to recall that the Law of 1 March 2019[1] and the Law of 22 January 2021[2] respectively enable the maintenance and circulation of securities by way of inscription in a distributed ledger and the issuance of such dematerialised securities through secured electronic registration mechanisms such as the DLT.

From an AML/CTF[3] standpoint, the Law of 12 November 2004 on the fight against money laundering and terrorist financing was amended by a law dated 25 March 2020 introducing a new status of "virtual asset service providers" which must be registered with the CSSF for such AML/CTF purposes.[4]

In this context of appetite for decentralisation and dematerialisation, the White Paper follows two FAQs (one related to **UCIs** and another one for **credit institutions**) published in November and December 2021 by the CSSF in relation to virtual assets. These FAQs emphasise the need for professionals to carry out a case-by-case assessment of the specific risks related to investments in, and services provided in relation to, such types of assets.

Please see our other **publication** for more information about the FAQ concerning UCIs.

Content of the White Paper

First of all, the White Paper, which is a non-binding document, agrees on the following definition for the DLT:

"*DLT is a technology allowing a network of independent and often geographically dispersed computers to update, share and keep a definitive record of data (e.g. information, transactions) in a common decentralised database in a peer-to-peer way, without the need for a central authority.*"

Then, the White Paper focuses on three main aspects:

- Explanatory developments related to the identification of the main components of a DLT and the different types of DLT;
- Indication of the roles and responsibilities of the different players in the use of the DLT such as the DLT developers or the infrastructures service providers;
- Emphasis on the fact that entities should weigh up the risks that involve the use of a DLT against the benefits.

From a practical standpoint, the White Paper ends with an appendix summarising all DLT-specific key questions and considerations, some of which have legal or contractual implications.[5]

1. Amending the Law of 1 August 2001 on the circulation of securities.
2. Amending the Law of 5 April 1993 on the financial sector and the Law of 6 April 2013 on dematerialised securities.
3. Anti-Money Laundering and Counter Terrorist Financing.
4. See: **https://www.cssf.lu/en/registration-vasp/**.
5. Noting in particular that performance of certain services may trigger the need to obtain additional or different licences.

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.