ELVINGER HOSS PRUSSEN

ELVINGER HOSS
LUXEMBOURG LAW

ICT, IP, media and data protection
NEWS

WELCOME TO THE 1ST EDITION OF OUR ICT, IP, MEDIA AND DATA PROTECTION NEWS

TABLE OF CONTENTS

WELCOME TO EHLO

EHLO is a new source of Luxembourg legal knowledge on information and communication technologies, intellectual property, media and data protection compiled by our lawyers working on a day to day basis in these areas of practice.

Our dedicated team closely follows the developments and ongoing emergence of new directives, laws and regulations as well as the increasing number of case law and guidance specifying the application in practice of the legal and regulatory landscape.

We are keen to share valuable information, which we deem of interest to you in easy to read format. We are of course available to expand on a given subject, upon request.

EHLO is not intended to replace our firm's general monthly Newsletter (to which you must subscribe if you wish to receive **EHLO**), but to supplement it by disseminating specific information and news in a reactive manner for these dedicated areas of practice.

Some topics with respect to information and communication technologies, intellectual property, media and data protection may be more extensively developed in the firm's general monthly Newsletter.

EHLO will be published at a varying frequency depending on the news, recent developments on a specific subject or growing interest on a specific point of interest.

For its launch, **EHLO** returns in the form of a retrospective on some key legal events of the year 2019.

Your ICT, IP, media and data protection team at Elvinger Hoss Prussen.

LINDA FUNCK
Partner
Tel: +352 44 66 44 5162
lindafunck@elvingerhoss.lu

Linda is active in the field of ICT and data protection, privacy, media and e-commerce law. She also has a broad experience in corporate law, financing and merger and acquisition transactions.

GARY CYWIE
Partner
Tel: +352 44 66 44 5162
garycywie@elvingerhoss.lu

Gary specialises in technology matters, data protection, internet and e-commerce. He also focuses on IT outsourcing in the financial sector and commercial contracts.

EMMANUÈLE DE DAMPIERRE
Senior Associate
Tel: +352 44 66 44 5158
emmanueledampierre@elvingerhoss.lu

Emmanuèle specialises in all areas of IP law (advisory and litigation work). She is also active in the field of ICT and data protection.

JONATHAN DAHMOUN
Senior Associate
Tel: +352 44 66 44 5157
jonathandahmoun@elvingerhoss.lu

Jonathan specialises in data protection, internet and e-commerce. He also deals with IT outsourcing, telecom and IP law.

MARIE BERNIER-RICHARD
Associate
Tel: +352 44 66 44 5176
mariebernierrichard@elvingerhoss.lu

Marie is involved in particular in data protection, IP and technology matters.

ANTHONY FAVIER
Associate
Tel: +352 44 66 44 5136
anthonyfavier@elvingerhoss.lu

Anthony provides legal advice in data protection matters, technology and media laws.

ICT

Developments of the CJEU on the concept of *electronic communications service*

In two judgments issued during summer 2019, the Court of Justice of the European Union ("**CJEU**") provided guidance regarding the qualification of a service as an "electronic communications service" with the meaning set out under Article 2(c) of Directive 2002/21/EC on electronic communications networks and services ("**Framework Directive**").

The CJEU indeed held different positions according to the nature of the services provided to end-users. It established that a "VoIP" service, such as Skype, could be seen as an electronic communications service, but not a web-based emailing service, such as Gmail.

The Framework Directive will be repealed with effect from 21 December 2020 due to the entry into force of Directive 2018/1972 establishing the European Electronic Communications Code, which relies on new concepts and (updated) definitions of electronic communications services.

For more developments with regard to those two cases, have a look at our article: **here**.

Liability of hosting service providers for defamation under e-Commerce Directive (Facebook)

On 3 October 2019, the CJEU made an important decision in case C-18/18 with respect to the liability of hosting service providers and whether they may be ordered to remove or block access to content that they store.. As a reminder, hosting service providers are subject to a specific liability regime regarding the information they transmit or store for their clients, but of course they remain subject to court injunctions. Accordingly, the CJEU decided that a host provider, in this instance Facebook, may be ordered to remove or to block access to information which was published on its social network, the content of which was identical to information previously declared to be unlawful.

Such an injunction would also be valid for equivalent (but not identical) content, to the extent that such content would remain essentially unchanged compared to the content previously declared unlawful and that the host provider is not required to carry out an independent assessment of that content to determine whether it is unlawful. Indeed, host service providers cannot be subject to a general obligation to monitor information they store or to actively search unlawful content, except in limited circumstances (e.g. under Luxembourg law, where necessary to safeguard national security or for the prevention, detection and prosecution of criminal offences).

The liability regime of host providers is governed at European level by Articles 14 and 15 of the Directive 2000/31/EC on e-Commerce. This liability regime was transposed into Luxembourg law under Articles 62 and 63 of the Law of 14 August 2000 on e-Commerce. Under this regime, hosting providers are not liable for information they stored if they do not have actual knowledge of their illegal nature or if they act expeditiously to remove or disable access to that information as soon as they becomes aware of it.

This may also interest you :

- CJEU "Fashion ID" case: the operator of a website embedding a social media "Like" button can be a controller jointly with the social media editor
- CJEU limits the de-referencing right to the EU territory

- Guidelines on the "right to be forgotten" in the specific case of online search engine
- Guidelines on data protection by design and by default

E- Commerce – Luxembourg Electronic signature regime to fully aligned with eIDAS Regulation

On 1 March 2019, the Luxembourg government approved a **draft law** to amend the Law of 14 August 2000 on e-Commerce. The draft law intends to align the current Luxembourg regime on electronic signatures stemming from the e-Commerce law with the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation). As of today, electronic signatures are governed in Luxembourg by the e-Commerce law and the directly applicable eIDAS Regulation. Aligning the definitions and criteria of electronic signatures will clarify the situation in practice and therefore increase trust in the use of electronic signatures in Luxembourg. The draft law has been submitted to the Chamber of Deputies. We will report with any noteworthy updates.

This may also interest you :

- New law on sanctions against geo-blocking discriminations
- Harmonisation of national consumer laws: New directives

DATA PROTECTION

CJEU *Fashion ID* case: the operator of a website embedding a social media *Like* button can be a controller jointly with the social media editor

On 29 July 2019, the Court of Justice of the European Union ("**CJEU**") rendered its judgment in the "Fashion ID" case (C-40/17).

The CJEU retained a broad concept on joint-controllership with regard to the processing of personal data due to the use of social media tools like certain embedded buttons. According to the CJEU, a website operator using such embedded features can be seen as acting as controller, jointly with the social media editor (i.e. Facebook), as these buttons permit the transmission of personal data (such as IP addresses) to the social media editor.

This decision shall be read in conjunction with previous decisions rendered by the CJEU in 2018, in particular one where an administrator of a Facebook page was considered as a joint-controller with Facebook (case C-210/16).

You may wish to read our full article regarding this case **here**.

This may also interest you :

- CJEU limits the de-referencing right to the EU territory
- Liability of hosting service providers for defamation under e-Commerce Directive (Facebook)

Schrems II case: EU to U.S. transfers of personal data challenged

Following Schrems I case (C-362/14 of 6 October 2015), which invalidated the Safe Harbour Privacy Principles, another legal action filed by Max Schrems challenges the EU to U.S. personal data transfers made by Facebook on the basis of the Standard Contractual Clauses approved by the European Commission (the "SCCs"). According to Mr. Schrems, such transfers infringe the EU data protection law as they allow U.S. authorities to access his personal data. On 19 December 2019, the Advocate General observed that the SCCs used by controllers to transfer personal data to processors established in third countries were themselves valid under the EU data protection law.

For more information on the procedure and/or the Opinion of the Advocate General, please have a look at our article: **Schrems II case: EU to U.S. transfers of personal data challenged**.

Elvinger Hoss Prussen will of course inform you of the outcome of the decision of the CJEU

This may also interest you :

- Data Protection - Consequences of a no-deal Brexit on personal data transfers to the UK
- EDPB published standard clauses for (sub-)processing activity

EU Entities can continue to transfer personal data within the Privacy Shield framework

According to the European Commission's **report**, the EU-U.S. Privacy Shield continues to ensure an adequate level of protection for personal data transferred to certified U.S. companies, as **listed** by the U.S. Department of Commerce. As a reminder, the Privacy Shield decision has been operational since 1 August 2016 and is subject to annual reviews by the European Commission, which took place respectively in September 2017 and October 2018 and 2019.

The third annual review (2019) highlights the improvements in the functioning of the Privacy Shieldframework, which as of today include more than 5,000 U.S. companies. The European Commission still concludes that additional concrete steps need to be taken to ensure better functioning in practice, including timing for the re-certification process during which U.S. companies remain on the Privacy Shield "active" list, the pro-active monitoring of the U.S. companies on more substantive obligations, such as the accountability for onward transfer principles, enlarging the scope of search for detecting false claims, and the development of guidance regarding the processing of human resources data.

This may also interest you :

- Schrems II case: EU to U.S. transfers of personal data challenged
- Data Protection - Consequences of a no-deal Brexit on personal data transfers to the UK

CNPD annual activity report 2018

On 18 September 2019, the Commission Nationale pour la Protection des Données (the "**CNPD**") (i.e. the Luxembourg data protection supervisory authority) published its annual activity report for 2018 and presented its key figures regarding notably information requests, complaints, data breaches, prior consultation regarding data protection impact assessments (DPIA), control, audits and on-site inspections, and sanctions. The key figures provided by the CNPD demonstrate that individuals become more aware of their rights and related obligations under the GDPR. However, the CNPD has not imposed any administrative fines so far. See more information **here**.

CJEU limits the de-referencing right to the EU territory

On 24 September 2019, the Court of Justice of the European Union ("**CJEU**"), following Advocate General(the "**AG**") Szpunar's Opinion, circumscribed the territorial scope of the de-referencing right to the European Union in the case C-507/17 Google LLC (successor in law to Google Inc.) v Commission nationale de l'informatique et des libertés (CNIL). The de-referencing is the right of individuals to request from online search engine operators that they remove information concerning them from the list of results displayed following a search on their name, the results of which are based on information indexed by the search engine on the internet.

According to the CJEU, the operator of a search engine is not required by EU law to carry out a dereferencing on all versions of its search engine, but only the versions implemented in all the Member States.

De-referencing beyond EU borders is not an obligation or a prohibited practice for search engine operators according to the Court. It underlines that the authorities of Member States remain competent to balance the right to privacy and protection of personal data on one hand and the freedom of information on the other hand and, where appropriate, to order the concerned operators of search engine to de-reference the information on all versions of their search engine.

This may also interest you :

- CJEU "Fashion ID" case: the operator of a website embedding a social media "Like" button can be a controller jointly with the social media editor
- Guidelines on the "right to be forgotten" in the specific case of online search engine

Guidelines on the *right to be forgotten* in the specific case of online search engine

The EDPB published its **Guidelines 5/2019** on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1) as adopted on 2 December 2019.

These Guidelines have been adopted as a consequence of the increase in the number of complaints filed by data subjects against the refusal by search engine providers to delist links displayed as a result in their search engine and directing to website(s) publishing information concerning such data subjects.

As a reminder, the "Costeja" judgment of the CJEU of 13 May 2014 (aka Google Spain case)[1] confirmed the existence of the so-called "right to be forgotten", which was already granted under Directive 95/46/EC as the right to object and right to erasure. Such rights are now provided under Articles 17 and 21 of the GDPR and may be referred to as the "right to request delisting" in the specific case of search engines.

The Guidelines highlight the possible grounds for requesting delisting from a search engine list of results as well as the possible exceptions to such a right.

They are now subject to public consultation until 5/2/2020 where the EDPB welcomes any comment from the public.

This may also interest you :

- CJEU limits the de-referencing right to the EU territory
- Guidelines on the territorial scope of the GDPR
- Guidelines on data protection by design and by default

1. CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

Consent requirements regarding cookies (Planet49 case) (Advocate General)

On 21 March 2019, Advocate General Szpunar ("**AG**") issued some clarifications about consent requirements with regard to cookies in the Planet49 case pending before the Court of Justice of the European Union (**Case C-673/17**, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.).

The facts: before hitting the participation button of a promotional online lottery organised by Planet49, the user had to enter his name and address and, beneath these fields, there were two sets of checkboxes accompanied by explanatory texts. One required the user to consent to cookies being installed on their computer (by unticking the box) while the other required the user to agree to being contacted by a certain number of firms for promotional offers (by ticking the box).

Consent is defined in Article 4(11) of the General Data Protection Regulation 2016/679 ("**GDPR**"), as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The AG, while applying Directive 2002/58/EC as amended ("**e-Privacy Directive**") either in conjunction with Directive 95/46/EC or with the GDPR (respectively for situations before and after the 25 May 2018), has advised regarding 'cookies checkbox', that there is no valid consent in a situation such as the case at hand "where the storage of information, or access to information already stored in the user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his consent and where consent is given not separately but at the same time as confirmation in the participation in an online lottery". Indeed, according to the AG, preticked boxes do not provide a guarantee that users have read the information and have therefore given their consent freely. Moreover, there is no separate consent since decisions to participate in the lottery and consent to the installation of cookies were made simultaneously. Additionally, the user was not fully informed that participation in the lottery was not conditional upon giving consent to such installation and gaining access to cookies.

According to the AG, this interpretation is also valid whether or not the information stored or accessed constitutes personal data.

The AG, while applying transparency requirements and informed consent concept considered that since the average internet user would not be expected to have a high level of knowledge on how cookies work, the clear and comprehensive information that a service provider has to give to a user "implies that a user is in a position to be able to easily determine the consequences of any consent he might give". This means that the information must be clear, comprehensible and unambiguous for such an average internet user. To this end, the AG is of the opinion that when access to the cookies is granted to third parties, the clear and comprehensive information that a service provider must give to a user must include the information on that access as well as the duration of the operation of these cookies.

The Court will deliberate and make a judgement at a later date. Even though the judges are not bound by the AG's observations, the legal solution he suggests, offers them a certain direction to take into consideration.

Consent requirements regarding cookies (Planet49 case) (CJEU)

On 1st October 2019, the Court of Justice of the European Union ("CJEU") decided that a pre-checked box which users must deselect to refuse the storage and access to cookies on their terminal equipment is not a valid consent. Storing and accessing cookies therefore requires the Internet user's active consent.

In this case C-673/17 (Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V), the CJEU confirmed Advocate General Szpunar's Opinion issued on the 21st March 2019.

The Court also confirmed that the information to be provided to users must include the information whether or not third parties may have access to cookies as well as the duration of operation of such cookies.

For more information on the facts which led to this decision as well as details on the AG Opinion, you may wish to read our **article** published in May 2019.

This may also interest you :

- Interaction e-Privacy principles / GDPR

Guidelines on data protection by design and by default

The EDPB published its **Guidelines 4/2019** on Article 25 - Data Protection by Design and by Default ("**DPbDD**") as adopted on 13 November 2019 (the "**Guidelines**"). The Guidelines give an in-depth analysis of the DPbDD requirements by reviewing one by one each condition provided by Article 25. They also focus on the controllers' accountability to demonstrate that appropriate measures and safeguards have been implemented to ensure that the data protection principles (transparency, lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality) are effective in practice and protect the rights and freedoms of data subjects.

The EDPB reminds practitioners that DPbDD is a requirement for all controllers, independent of their size, including small local associations and multinational companies alike. However, the Guidelines may be useful to processors and technology providers who are interested in creating GDPR-compliant products and services for controllers, which can turn into a competitive advantage in the market. On the other hand, controllers are discouraged from using providers whose technology is not compliant with DPbDD because accountability for lack of implementation thereof is on the controllers.

The Guidelines also state that DPbDD must be taken into account from the initial stages of a planned processing operation to allow controllers to correctly implement the data protection principles and provide illustration and key DPbDD elements for each data protection principle.

It is also stated that certification mechanisms may be used as an element to demonstrate compliance with the DPbDD requirements and be used by both controllers and processors to enhance trust in the processing of personal data.

The Guidelines are subject to public consultation until 16/01/2020 where the EDPB welcomes any comment from any interested person.

This may also interest you :

- Guidelines on the "right to be forgotten" in the specific case of online search engine
- Guidelines on the territorial scope of the GDPR

Guidelines on the territorial scope of the GDPR

The EDPB published its finalised **Guidelines 3/2018** on the territorial scope of the GDPR on 12 November 2019 (the "**Guidelines**"). The purpose of the Guidelines is to help controllers, processors and supervisory authorities in determining whether a particular processing activity falls within the territorial scope of the GDPR. Indeed, for the main criteria of Article 3 of the GDPR (the "establishment" and the "targeting" criteria),

the EDPB developed an approach for determining whether or not the GDPR applies to a specific data processing activity. The Guidelines also provide some useful information regarding the (non-)designation of a representative for controllers or processors not established in the EU as well as its related obligations and responsibilities.

The following observations can be made regarding the updated Guidelines:

- the **application of Article 3** aims at determining whether a **particular processing activity (on a processing-by-processing basis), rather than a (legal or natural) person** falls within the scope of the GDPR. Therefore, for the same controller/processor, certain processing of personal data might fall within the scope of the GDPR, while other processing might not (we underline);
- where a non-EU controller or processor '***inadvertently or incidentally***' targets its goods or services at a data subject located in the EU, such processing of personal data will not fall within the scope of the GDPR.
- still on the **targeting criterion**, regarding **processors not established in the EU**, the EDPB specifies that their processing activities can fall within the scope of the GDPR if they are 'related' to the targeting activities of the controller.
- the EDPB emphasizes that the **representative** is not liable in place of the non-EU controller or processor that it represents. The representative's direct liability is limited to its direct obligations referred to in Article 30 (record-keeping) and Article 58(1)(a) (respond to information requests from the supervisory authority) of the GDPR. The EDPB also specifies that the role of a representative in the EU is not compatible with the role of a Data Protection Officer.

This may also interest you :

- Guidelines on the "right to be forgotten" in the specific case of online search engine
- Data Protection - Consequences of a no-deal Brexit on personal data transfers to the UK
- Guidelines on data protection by design and by default

EDPB published standard clauses for (sub-)processing activity

The European Data Protection Board ("**EDPB**") delivered a positive opinion on the **Article 28 Standard Clauses** adopted on 10 December 2019 by the Danish Supervisory Authority. The clauses intend to serve as a standard processing agreement between controllers and processors for the purpose of Article 28.3 of Regulation 2016/679 (GDPR). They contain sections to be filled in by the parties (e.g. controller and processor), options to be selected (e.g. general or specific authorisation to use sub-processors) and appendices to be completed (e.g. information about processing, list of sub-processors, instructions for processing) so that they can be adapted to the circumstances at hand.

The EDPB noted that the Danish Supervisory Authority will be able to refer to the Standard Clauses as a model of processing agreement pursuant to Article 28.8 of the GDPR. Parties may still add other clauses provided that they do not contradict the Standard Clauses or prejudice the rights of the data subjects, but in case of modification, the parties will not be deemed to have implemented a standard agreement adopted by a Supervisory Authority.

The Standard Clauses adopted by the Danish Supervisory Authority must not be confused with the current European Commission's standard contractual clauses or the expected standard data protection clauses of Article 46 of the GDPR covering personal data transfers and cannot thus be relied on as an appropriate

safeguard for transferring personal data to processors located outside the European Economic Area. Therefore, such transfers still require compliance with Chapter V of the GDPR in addition to the use of the Danish Standard Clauses.

This may also interest you :

- Data Protection - Consequences of a no-deal Brexit on personal data transfers to the UK
- Schrems II case: EU to U.S. transfers of personal data challenged
- EU Entities can continue to transfer personal data within the Privacy Shield framework

Data Protection - Consequences of a no-deal Brexit on personal data transfers to the UK

Several administrations released information on the consequences of a no-deal Brexit. So did the National Data Protection Commission in Luxembourg (CNPD) in a "Brexit" report published on their website. EU businesses subject to the GDPR should review their personal data flows and, if appropriate, review their situation to ensure that personal data transferred to the UK will still be made in compliance with EU legislation in the event of a no-deal Brexit. In most cases, the soundest alternative would generally be for EU-based data exporters to enter into Standard Data Protection Clauses (also known as EU Model Clauses) with the relevant UK data importers. Please **read our analysis here**.

This may also interest you :

- Schrems II case: EU to U.S. transfers of personal data challenged
- EDPB published standard clauses for (sub-)processing activity
- EU Entities can continue to transfer personal data within the Privacy Shield framework

Data Protection - CNPD provides further Guidance: Processing operations requiring a DPIA

The General Data Protection Regulation ("**GDPR**") provides that where a type of processing of personal data is likely to result in a "high risk" to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out a data protection impact assessment ("**DPIA**"). In this context, the GDPR commands national data protection authorities to establish and publish a list of the kind of processing operations that are subject to this requirement for a DPIA. With its **deliberation 34/2019 of 6 March 2019**, the Luxembourg Data Protection Authority ("**CNPD**") therefore published a list of processing operations requiring the prior performance of a DPIA specifying that such a list is not to be seen as exhaustive.

This may also interest you :

- Guidelines on the territorial scope of the GDPR
- Guidelines on the "right to be forgotten" in the specific case of online search engine
- Guidelines on data protection by design and by default

Interaction e-Privacy principles / GDPR

On 10 January 2017, the EU Commission issued a **proposal** for a Regulation on the respect for private life and the protection of personal data in electronic communications ("**e-Privacy Regulation**") which aims to replace the current legal framework established under Directive 2002/58/EC ("**e-Privacy Directive**").

The e-Privacy Directive, as implemented into the national legislations of the EU Member States, provides special privacy rules for electronic communications services and therefore regulates activities such as the use of cookies and unsolicited electronic communications.

The proposal for the e-Privacy Regulation intends to further harmonize the rules on electronic communications across all Member States by defining better and clearer rules on tracking technologies, in particular by taking into account the principles and requirements deriving from the General Data Protection Regulation 2016/679 ("**GDPR**").

In terms of timing, the EU institutions were initially aiming to adopt the e-Privacy Regulation by 25 May 2018, i.e. the date of entry into application of the GDPR. This was then post-poned until the end of 2018. This timing would have established a comprehensive framework on the matter at hand. However, the adoption of the e-Privacy Regulations has taken longer than expected due to the huge economic and financial stakes at hand. Indeed, discussions are still ongoing within the Council and the proposal has not made it yet to the first reading at the Parliament.

Meanwhile, following a request from the Belgian data protection authority, the European Data Protection Board ("**EDPB**") adopted on 12 March 2019 **Opinion 5/2019** on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities ("**Opinion**").

The Opinion recalls that certain processing activities may fall within the material scope of application of both the e-Privacy Directive and the GDPR. The EDPB nevertheless emphasises that, in accordance with the adage *lex specialis derogat legi generali*, the general rules set out in the GDPR shall apply in the absence of specific provisions governing a particular processing operation or set of operations, in particular in relation to the rights granted to data subjects.

Furthermore, the Opinion recalls that the GDPR itself recognizes the complementary role of the e-Privacy Directive in its Article 95 which states that the GDPR should not impose additional obligations on electronic communications service providers which are subject to specific obligations with the same objective set out in e-Privacy Directive. A concrete example of such potentially duplicated obligations would be in case of personal data breach notification obligations as prescribed under both legal instruments. The result of applying Article 95 of the GDPR is that once a breach notification is made under the e-Privacy Directive (as implemented into national law), there is no need for a separate data breach notification under the GDPR.

The EDPB finally states that where a subset of a processing falls within the scope of the e-Privacy Directive, this does not necessary limit the competence of data protection authorities as set out under the GDPR.

This may also interest you :

- CJEU limits the de-referencing right to the EU territory
- Consent requirements regarding cookies (Planet49 case) (CJEU)

INTELLECTUAL PROPERTY

Trademark and bad faith

Be aware: The following practice is not authorised (at least for EU trademarks)

Re-filing identical marks a few years after the first filing with a wider list of goods and services to avoid having to prove the use of the brand at the end of the five-year grace period.

(Decision of one of the EUIPO's Boards of Appeal (Case number: R1849/2017-2): partial invalidation for bad faith).

Which requirements for a finding of bad faith?

On 12 September 2019, the Court of Justice of the European Union ("CJEU") has decided in its case C 104/18t that when seeking a declaration of invalidity on the grounds of bad faith, there is no need for the applicant to have similar/identical goods and services.

This may also interest you :

- Trademark – European Reform implemented in Luxembourg
- Adoption of new European copyright directive

Trademark – European Reform implemented in Luxembourg

On 1 March 2019, the amended Benelux-Convention on Intellectual Property ("BCIP") entered into force to be in line with the European Trade Marks Directive (Directive 2015/2436).

We have listed below the most important changes:

The requirement of graphical representation has been removed: as a consequence, it is now possible to register non-conventional trademarks such as sound marks, motion mark or multimedia marks.

Absolute grounds for refusal are extended to all signs consisting exclusively of the shape or another characteristic that is defined by the nature of the goods, or is necessary to obtain a technical result or gives substantial value to the goods. This expands the grounds for cancellation.

The position of the rights holder is reinforced in case of comparative advertising, use of a trademark in a company name and counterfeit goods in transit.

A regime for registration of certification marks has been introduced.

It is now expressly stated in the BCIP that products and services must be described with sufficient clarity and precision.

For more information on the modifications of the BCIP modifications, please contact our ICT/IP/Data Protection department.

This may also interest you :

- Trademark and bad faith
- Adoption of new European copyright directive

Adoption of new European copyright directive

As already indicated **here** in July 2019, the Directive on copyright and related rights in the Digital Single Market[1] (the "**New Copyright Directive**") was finally adopted on 17 April 2019 after months of negotiation.

While the European Commission describes the New Copyright Directive as the "*right balance between the interests of all players – users, creators, authors, press – while putting in place proportionate obligations on online platforms*"[2], some Member States – among which is Luxembourg – have disapproved the proposed text of the New Copyright Directive and have considered that it is "*a step back for the Digital Single Market rather than a step forward*"[3]. Those Member States have in particular denounced the lack of legal clarity of the New Copyright Directive.

Please note that Member States shall transpose the New Copyright Directive into their national legislation by 7 June 2021. It is likely that further discussions will start within the Member States at the time of transposition of the New Copyright Directive.

This may also interest you :

- Trademark and bad faith
- Trademark – European Reform implemented in Luxembourg

1. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

2. European Commission – Statement, 26 March 2019, Statement 19/1839

3. Council of the European Union, Joint statement by the Netherlands, Luxembourg, Poland, Italy and Finland, 15 April 2019, 7986/19 ADD 1 REV 2 (interinstitutional File: 2016/0280(COD))