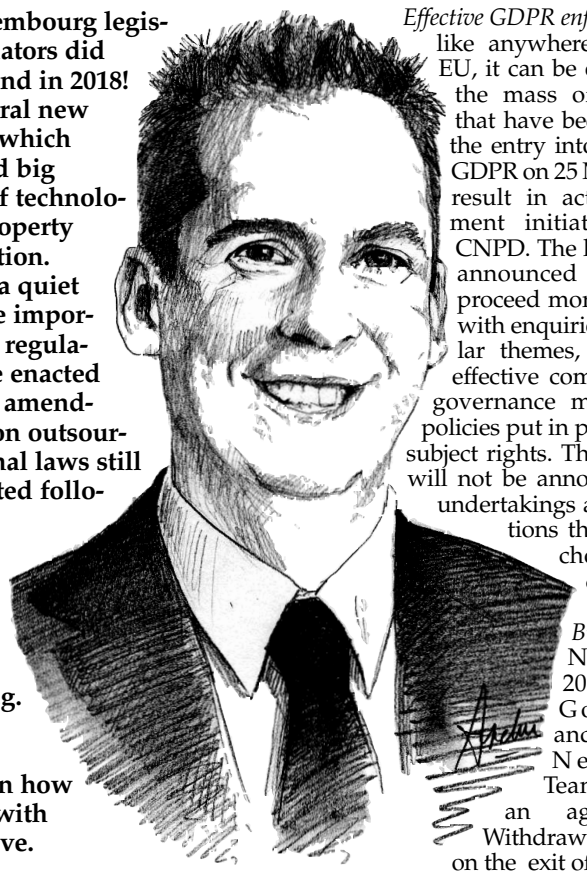
2019: another challenging year of changes in Technology & IP law

The EU and Luxembourg legislators and regulators did not just sit around in 2018! They brought us several new laws and regulations which have already triggered big changes in the field of technology and intellectual property ("IP") law and regulation. And 2019 will not be a quiet year either since some important pending law and regulation proposals will be enacted (ePrivacy Regulation, amendments to CSSF rules on outsourcing) and some national laws still need to be implemented following the adoption of European directives (NIS and Trade Secret directives). Furthermore, some news trends continue to gain importance (e.g. artificial intelligence, block chain, etc.) and need a clear answer on how they should be dealt with from a legal perspective.



Another focus will most certainly lie on the enforcement of some legal instruments that came into force in 2018: we will see the first real enforcement initiatives with respect to the GDPR and the Geoblocking Regulation (EU) 2018/302. Last but not least, there is of course the Brexit and its potential impact on data protection regulation and IP rights.

In this article, we will get you up to speed on these legislative and regulatory changes and challenges. Enjoy and happy new year!

GDPR: Luxembourg specific regimes, enforcement and Brexit

Luxembourg specific provisions. The EU General Data Protection Regulation 2016/679 (the «**GDPR**») is applicable in the EU since 25 May 2018. As the GDPR is an EU regulation, its provisions are directly applicable in Luxembourg, yet the GDPR also leaves some room for the adoption of specific national rules. In this context, the Luxembourg law of 1 August 2018 on the organisation of the National Commission for Data Protection (*Commission Nationale pour la Protection des données*, the "**CNPD**") entered into force on 20 August 2018 («**Luxembourg GDPR Law**») and notably introduced specific provisions for personal data processing for journalistic, research and healthcare purposes. Such law however proves challenging for both the research community which faces quite strict conditions and the insurance sector which needs to obtain the consent of the data subjects to process their health related data.

Luxembourg DPIA list. The Luxembourg list of critical data processing activities that always require a so-called data protection impact assessment, is due to be published at the beginning of 2019.

Employee monitoring. This Luxembourg GDPR Law has also amended Article L. 261-1 of the Luxembourg Labor Code which lays down the conditions for monitoring at the workplace by rendering the use of such monitoring easier for employers. This new regime liberalises somewhat the purposes for which the use of monitoring techniques at the workplace for employers in Luxembourg is allowed and abolishes the CNPD authorisation requirement. Employers are still subject to an increased information obligation to both the concerned employees and the staff delegation. They further have to comply with the general obligations resulting from the GDPR (e.g. internal records keeping, prior impact assessment).

Certification scheme. In 2019, the CNPD will adopt its certification scheme and accredit the first certification bodies under such scheme which will undoubtedly give a boost to undertakings and organisations to demonstrate their compliance with the GDPR on the basis of an official certification.

Further EBPD guidance. The European Data Protection Board, the successor of the Article 29 Working Party, which regroups representatives of all EU data protection authorities, already issued guidance on important topics in 2018, such as consent, transparency and territorial scope. Further guidance can however be expected in 2019 and, more particularly, on the territorial scope of the GDPR (Article 3), on the Luxembourg DPIA lists, on the Commission's Japan Adequacy Decision, on codes of conduct, etc.

Effective GDPR enforcement. Just like anywhere else in the EU, it can be expected that the mass of complaints that have been filed since the entry into force of the GDPR on 25 May 2018 will result in actual enforcement initiatives of the CNPD. The latter has also announced that it will proceed more proactively with enquiries on particular themes, such as the effective compliance with governance measures and policies put in place and data subject rights. These enquiries will not be announced to the undertakings and organisations that have been chosen in this context.

Brexit. On 14 November 2018, the UK Government and the EU Negotiation Team published an agreed draft Withdrawal Agreement on the exit of the UK from the EU, accompanied by a draft outline of the Political Declaration on the future of the UK-EU relationship. The Withdrawal Agreement currently provides that, after the end of the transition period (December 2020), the UK must continue to apply the EU data protection rules until the EU has established, by way of a formal adequacy decision, that the personal data protection regime of the UK provides data protection safeguards which are «essentially equivalent» to those in the EU. It remains to be seen whether the UK parliament will accept the Withdrawal Agreement or whether we are heading towards a hard Brexit, in which event this formal adequacy decision should be adopted sooner and as early as possible after the effective exit date in order to guarantee the flow of personal data from the EU/EEA towards the UK.

Privacy and electronic communication (ePrivacy)

The draft regulation concerning the respect for private life and the protection of personal data in electronic communications (draft regulation 2017/0003 (COD) or «**ePrivacy Regulation**») is still under discussion between the EU institutions and EU Member States within the Council of the EU. The ePrivacy Regulation aims at providing an alignment with the new standards of the GDPR and increasing trust in and the security of digital services.

The ePrivacy Regulation will have an impact on the confidentiality of electronic communications, direct marketing practices, website audience measurement and the settings for tracking technologies (including the use of cookies). Several key elements of the regulation are still under discussion at this stage, yet there is hope that the ePrivacy Regulation will be adopted before the European Parliament elections in May 2019. If not, the entry into force of this long awaited piece of legislation will be further delayed. To be continued ...

Implementation of Directive (EU) 2016/1148 on security of network and information systems

Directive (EU) 2016/1148 on security of network and information systems (the "**NIS Directive**") is the first piece of European legislation on cybersecurity aiming at achieving a high common level of security of network and information systems within the EU.

EU Member States will need to adopt a national strategy on the security of network and information systems and also have to designate national competent authorities, single points of contact and computer security incidents response teams with tasks related to the security of network and information systems. Operators of essential services and digital service providers will also be subject to security and notification requirements.

The NIS Directive had to be implemented by all EU Member States by 9 May 2018. The EU Member States then had six months to identify operators of so-called «essential services» (e.g. entities active in the sector of transport, health, energy, digital infrastructure, credit institution, etc.) by 9 November 2018. The Luxembourg implementing law is however still under discussion (bill of law n°7314) but is expected to be enacted soon.

Free flow of non-personal data

The Regulation (EU) 2018/1807 on the free flow of non-personal data («**FFD Regulation**») in the EU prohibits data localization requirements, unless they are justified on grounds of public security. It must be noted that «data localization requirements» is defined in a rather broad manner and encompasses any kind of obligation that imposes the processing of non-personal data in the territory of a specific EU Member State or any hindrance of the processing of non-personal data in any other Member State.

As from 29 May 2019, it will be prohibited for national legislators and regulators to adopt new data localisation requirements unless they are justified on grounds of public security. EU Members States have until 30 May 2021 to repeal the current national data localisation requirements that are not justified on grounds of public security. It goes without saying that the FFD Regulation is a challenge for the regulation of the Luxembourg financial sector, which traditionally makes the processing of client related data abroad subject to rather strict conditions.

E-evidence

In 2019, a framework on e-evidence will be adopted at EU level. This framework includes the draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and would *inter alia* create a EU order allowing a judicial authority in one EU Member State to obtain electronic evidence directly from an electronic communication, information society or internet domain name and IP numbering service provider in another EU Member State in criminal matters.

Outsourcing in the Luxembourg financial sector

In 2018, the Luxembourg legislator adopted a law which clarified the rules on outsourcing in the financial and insurance sectors and the possibility to obtain customer acceptance in this respect. Just before, in 2017, the CSSF harmonised its outsourcing rules for all financial and payments institutions alike and introduced a specific set of rules for IT related outsourcing based on a cloud infrastructure. Furthermore, in August 2018 the CSSF also subjected fund managers to its cloud regulations.

In 2019, we may expect that the CSSF continues with the enforcement of its outsourcing and cloud related regulations as it came to the conclusion that many financial institutions and service providers failed to comply with the compulsory authorisation and notification requirements that exist in this context.

For 2019, we may furthermore expect that the CSSF will amend its outsourcing regulations so as to synchronize them with the outsourcing guidelines of the European Banking Authority («EBA») which are due to be revamped in Q1 of 2019. The proposed guidelines of the EBA integrate the recommendation on outsourcing to cloud service providers that was published by the EBA at the end of 2017 and wish to apply to all financial institutions that are within the scope of the EBA's surveillance mandate: credit institutions and investment payment institutions and electronic money institutions. The proposed guidelines seek to render the concerned companies accountable for providing the local regulators with sufficient information regarding the so-called «material» outsourcing agreements engaged. Such information must contain *inter alia* the «risk analysis for the material activities to be outsourced» regarding notably the criticality of the concerned outsourced activity. The proposed guidelines furthermore foresee in a notification obligation to the local regulators and an obligation to keep a record of all material (or not) outsourced activities and to provide a copy of it upon request.

The CSSF has already announced that these guidelines will be duly taken into account and that it will adapt its cloud regulations so that some conditions (e.g. in terms of business continuity requirements) are better aligned with the reality and in order to build in more flexibility for non-material outsourcing activities based on a cloud infrastructure (e.g. no authorisation required). Another document to take note of is the guidance that the CSSF has provided on the use of artificial intelligence in the financial sector (e.g. when using chatbots or in the context of fraud detection).

Payment Services: the full implementation of open banking!

After the implementation in Luxembourg of the EU Payment Services Directive («**PSD 2**») through the Law of 20 July 2018, the next regulatory deadlines in the field of payment services are already around the corner. Establishments that are subject to PSD2 will soon have to comply with regulatory technical standards for strong customer authentication and common and secure open standards of communication («RTS») and the various EBA guidelines published in relation thereto. The RTS inter alia set out technical rules to be complied with to ensure that open banking is implemented by 14 September 2019. To do so, the European Commission requests the account servicing payment service providers to enable third party providers to test their «open banking interfaces» and to grant them access to relevant information by 14 March 2019 already. This year will thus create a new open banking market and enable account information service providers (AISP) and payment initiation service providers (PISP) to develop their activities, keeping in mind that banks may enter this market and will hence have to position themselves very quickly.

Geo-blocking

The Geo-Blocking Regulation (EU) 2018/302 addresses unjustified online sales discrimination or access to goods and services based on customers' nationality, place of residence or place of establishment within the internal market. It is applicable since 3 December 2018, but there is still a Luxembourg bill of law n° 7366 pending which will contain some provisions on the enforcement mechanism of this regulation (amongst others, a possibility to have a fast-track procedure on the merits to obtain the cessation of geo-blocking practices before the president of the commercial chamber of the Luxembourg District Court (*Tribunal d'arrondissement*)).

Collaborative economy: Luxembourg rules to be expected

Following several questions raised by some members of Parliament, the Luxembourg government is likely to come up with some legislative proposals in relation to the collaborative economy (organized via platforms such as Uber and Airbnb).

Portability

The Regulation (EU) 2017/1128 on cross-border portability of online content services in the internal market is applicable since 20 March 2018. An online content service provider must now enable subscribers visiting another EU country to have access to its paid-for service in the same way as in their country of residence. This can be video on demand (e.g. Netflix, Amazon Prime, etc.), online TV, music streaming (e.g. Spotify, Deezer) or online game marketplaces.

Trade Secret Directive (EU) 2016/943: Luxembourg implementation

The Trade Secrets Directive (UE) 2016/943 harmonises the national laws in the EU countries against the unlawful acquisition, disclosure and use of trade secrets. The directive will streamline the scope of trade secret infringements and will set forth a clearer and more harmonised procedural framework for the enforcement of trade secrets. The remedies that are foreseen, are inspired by the IP Enforcement Directive (EC) 2004/48 and make that the protection of trade secrets becomes a regime that is quasi-equivalent to the traditional IP protection regimes. Furthermore, the directive provides for measures in in order to protect the confidentiality of trade secrets in the course of legal proceedings.

In principle, EU Member States should have implemented Directive 2016/943 by 9 June 2018. In Luxembourg, a bill of law (n°7353) is however still going through the legislative process. If adopted in its current version, the *Tribunal d'arrondissement* sitting in commercial matters (even when the parties are not merchants), will in principle be competent to hear trade secret protection claims. It will be able to pronounce *inter alia* the following measures: cessation or, as the case may be, the prohibition of the use or disclosure of business secrets, appropriate remedial measures with respect to the infringing property, destruction of all or part of any document, object, material, substance or electronic file that contains or materializes the trade secret. Claims for damages must be brought on the basis of the common competence rules.

Vincent WELLENS (picture), Avocat à la Cour
Partner, NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Faustine CACHERA, Avocat à la Cour
Associate, NautaDutilh Avocats Luxembourg S.à r.l.
faustine.cachera@nautadutilh.com