ALTANA
AVOCATS • PARIS

NEWSLETTER IP/IT

SEPTEMBER 2016

FOCUS

PERSONAL DATA: HAVE YOU ANTICIPATED THE CHANGES?

The European Union (the "EU") adopted a new **Regulation,** on 14 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation (EU) 2016/679). It will enter into force as of **25 May 2018**.

In order to best anticipate this Regulation's entry into force, we present below some of the key changes.

Territorial scope

Application of the Regulation will depend, in particular, on **(i)** the data controller or processor's **place of establishment** within the EU, whether or not the processing takes place in the Union, or **(ii) the location of the person** whose data is collected (within or outside of the EU zone) **and the activities related to the processing** (to the provision of goods or services in the Union to these individuals concerned or to the monitoring of these persons' behavior, to the extent that it is a behavior that took place within the Union).

Privacy by design and Privacy by default

The data controller must adopt internal rules as well as technical and organizational measures that comply with the **principle of the protection** of personal data **upon design** (of a service, software, etc.) (***Privacy by design***). This includes, for example, pseudonymising the data as soon as possible; guaranteeing transparency; allowing the person concerned to control the data processing.

These measures must also comply with the principle of the protection of personal data by default (***Privacy by default***) in order to guarantee that only the data necessary for each purpose is processed and allowing the user the possibility to expand the privacy parameters thereafter.

Accountability

The data controller must implement internal mechanisms and procedures allowing it to **demonstrate and prove compliance with the data protection regulations**.

The objective is to identify and document the measures the data controller puts in place in order to comply with the requirements resulting from the Regulation (keeping of a register, performance of impact assessments, etc.)

This **documentation obligation** will have considerable practical consequences for companies required to integrate it into their internal procedures, alert and train their different departments and centralize the information with one dedicated person.

The supervisory authority may verify compliance with these obligations at any time. Companies **will be obligated to notify** the supervisory authority of any data processing violation as soon as possible (maximum 72 hours) as well as the individuals concerned.

Profiling

The Regulation **formalizes this concept,** which it defines as any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance (health, interests, location, etc.).

Profiling cannot be done **without the consent** of the individual concerned, who must be able to oppose his or her profiling at any time. This right must be explicitly brought to the attention of the individual concerned, and be clearly presented separate from any other information.

New liability for processors

The Regulation initiates a **principle of processor liability.**

Processors will henceforth have their own obligations and obligations shared with the data controller. The two actors will be jointly liable towards the individual concerned when they participate in the same processing. This guarantees an effective remedy to the individual concerned.

Beyond the liability towards the individual concerned, the CNIL may also directly address the processor, audit of his activity and, if necessary, penalize it.

Strengthening of the obligation to inform

In addition to the information that already has to be provided by the data controller in accordance with the current regime, the data controller **will have to inform the concerned individual** of, among other things, his or her right to introduce a claim before a supervisory authority, the existence of decisions made automatically (such as profiling), the contact details of the Data Protection Officer if one is appointed, the source of the data when it has not been directly collected from the person concerned, etc.

A practical consequence that this reinforcement will have for companies is **the necessity to revise confidentiality policies** and other documents carrying this information which currently reference the right to access and rectification.

Obligation to designate a Data Protection Officer

The appointment of a "data protection correspondent" (known in French as the "*correspondant informatique et libertés*" or "CIL"), according to the terminology of the Law of 6 January 1978 is currently a power granted to data controllers.

The Regulation creates the requirement to **appoint a "Data Protection Officer" or "DPO"** in certain cases.

Therefore, among those who will be required to appoint a DPO are data controllers or processor whose core activities consist of processing operations that, due to their nature, scope and/or purposes, require regular and systematic large scale monitoring of the person concerned.

Companies should therefore determine if the nature of their activities enters into the scope of this definition and if, consequentially, they are subject to this new obligation.

Penalties

The Regulation provides a **considerable increase in the CNIL's authority to impose monetary penalties,** which could go up to 20 million Euros and 4% of the company's turnover.

The French draft bill for a "Digital Republic" began to **anticipate this increase in penalties** by the CNIL by raising the ceiling from 150 000 Euros to 3 million Euros. This bill should be adopted into law during the second half of 2016.

To learn more

Altana will be shortly organizing a **breakfast** on the theme of **Cybersecurity**, during which these points will be further developed from a practical perspective.

CASE LAW NEWS

Inclusion of "applicable law clauses" in E-commerce General Terms and Conditions

The Court of Justice of the European Union ("CJEU") was asked to give a preliminary ruling on **whether or not** a clause in the general terms and conditions of an e-commerce contract between a consumer and a professional that applies only the law of the country where the professional is established to the contract, **is abusive**.

The Court responded to this question by holding that such a clause can be abusive, **when it misleads the consumer, by giving the impression that only the law of this Member State** applies, without informing the consumer that he also benefits from protection from the law which would be applicable to him in the absence of this clause.

This solution echoes the decision of the Paris Court of Appeal on 12 February 2016, which characterized **the jurisdiction clause**

inserted in Facebook's General Terms and Conditions as abusive.

The granting of jurisdiction to the California courts would effectively create, according to the Court, practical difficulties and a cost of accessing the courts of a nature to dissuade the consumer from exercising any action.

CJEU – 28 July 2016, C-191/15 *Verein für Konsumenteninformation / Amazon EU SARL*

The communication on a court decision concerning a competitor

Two decisions have been rendered concerning the possibilities for a company to communicate on a judgement that sentences a competitor.

The Paris Court of Appeal found that **the sending** by a company **of an email to clients and prospects of a non-final judgement rendered against a competitor** is not sufficient to constitute an act of **disparagement and unfair competition**.

The sole communication of a court decision, which is in essence public, is not constitutive of an act of disparagement.

Inversely, the Commercial Court of Lyon considered that a company that sent **a truncated and erroneous court decision** concerning a competitor to a prospective client committed an act of disparagement.

CA Paris, Pôle 1, Ch. 2 - 16 June 2016
Commercial Court of Lyon – 22 June 2016

Liability of physical marketplaces as intermediaries

By a decision on 7 July 2016, the CJEU found that **a company that sublets sites,** where counterfeits are sold, in market halls must be considered as an **intermediary** in the meaning of Directive 2004/48.

The concept of intermediary can therefore apply to operators of both online and physical marketplaces.

The intermediary can be required **by court order to take certain measures aimed at putting an end to the acts of counterfeit** (facilitate the identification of the seller, suspend the author of the infringement of the intellectual property rights in order to avoid new infringements of this nature by the same merchant against the same trademarks, etc.).

The Court notes, however, that the intermediary cannot be subject to a permanent and **general monitoring** requirement because such court order would be excessively costly and create an obstacle for legitimate commerce.

CJEU – 7 July 2016, C-494/15 *Tommy Hilfiger Licensing e.a.*

Absence of protection against an imitation of an insufficiently distinctive commercial sign

A previous "Optical Center" franchisee sold his business. The assignee has since operated under the commercial sign "Optical Centre".

The company Optical Center, who used this name as its sign, subpoenaed the latter, considering that it infringed on its commercial name and that there existed a risk of confusion between the two.

Despite the possible resemblance between these terms, the Paris Court of Appeal rejected Optical Center's claims, **considering that the sign in question was not sufficiently distinctive** and, as it does not allow for the identification of a commercial origin, there exists no risk of confusion.

Optical Center also considered that the store imitated the **arrangement of the stores** created by the franchise network. This grievance was also dismissed by the Court, who considered that the arrangement in question was commonplace, because it is required by the nature of the business.

CA Paris, Pôle 5, Ch.1 – 24 May 2016

IN BRIEF

On 12 July 2016 the European Commission **adopted** the **Privacy Shield** Adequacy Decision. This text, which creates a new **framework** for the **transfers** of data between the European Union and the United States, will enter into effect upon its notification to each of the Member States. It will be applicable to companies which will be registered with the American authorities in charge of the implementation of the measure.

In a ministerial response on 12 July 2016, the Minister of State for Commerce, Trade, Consumption and Social Solidarity Economy stated that the practices of ***IP Tracking***, which allow e-commerce sites to change the prices depending on the internet user's behavior could be considered as **unfair and deceptive trade practices**, and/or in violation of personal data regulations.

PRACTICIONNER'S CORNER

PROTECTING THE COMPANY'S TRADE SECRETS

After the withdrawal, in February 2015, of the provision of the French draft bill "Macron Law" bearing on the protection of trade secrets, the European Union adopted a text allowing for a **special and harmonized protection** of these secrets.

The EU Directive 2016/943 on the protection of know-how and undisclosed business information (trade secrets) against unlawful acquisition, use and disclosure (the "***Trade Secrets Directive***") of 8 June 2016, entered into effect on **5 July 2016**.

Main provisions of the Trade Secrets Directive

The Trade Secrets Directive provides, in particular:

- A **definition** of the concepts of "trade secrets", and of their lawful and unlawful acquisition, use and disclosure;
- The **exceptions** in order to ensure the **freedom of expression and information**, and to protect **"whistleblowers"** acting for the purposes of general interest;
- As part of **judicial proceedings**, obligations of confidentiality, particularly for the parties and judicial personnel, to **preserve the secret**. Unless an exception is made, confidentiality must be respected **even after the proceedings have ended**.
- The types of **court orders and coercive measures** that may be ordered against an infringer;
- The rules for the **determining of damages** that could be granted to the aggrieved company.

Current protective measures for trade secrets

A two-year period is planned for the transposition of the Directive, which would be **9 June 2018**.

In the meantime, substantive law still provides companies different means to protect their trade secrets.

Criminal law punishes, for example, the **theft of information**, abuse of confidentiality, or the criminal act of an employee revealing an industrial secret.

Tort liability can also be engaged, **on the basis of unfair competition.**

It should be noted in this regard that the recent reform of contract law provides a **legal confidentiality** obligation for information obtained as part of **negotiations**.

It is also possible to stipulate confidentiality clauses in **employee employment contracts** and in contracts concluded with third-parties (service providers, suppliers, etc.)

The contractual provision of such an obligation allows, in particular, to precisely define the scope of information covered by confidentiality.

Preventative measures

Certain **organizational and technical measures** can be taken by companies in order to **prevent a violation** of their trade secrets.

Companies can **classify their data based on its sensitivity** and adopt corresponding technical protective measures.

Confidential information should be **clearly identified as such**, particularly by the persons who use it, by placing, for example, the

indication “confidential” on the documents or during the sending of emails.

Significant attention should also be paid during the **departure of an employee** or the change of service provider, and the technical measures should permit employer monitoring. These measures must, however, also comply with the legal provision of employment law and the protection of **employee’s privacy.**

FIRM NEWS

The IP-IT team, in collaboration with the Criminal Litigation team, will organize a breakfast on the **theme of Cybersecurity in November.**

The Firm is pleased to inform you of the **arrival of Marie Hindré,** as a Partner, to reinforce the Economic Law and Competition Department. We welcome her among us.

ALTANA
VOCATS • PARIS

45 rue de Tocqueville • 75017 Paris, France
Tel. : +33 (0)1 79 97 93 00
www.altanalaw.com

Altana IP /IT team

Pierre Lubet / **plubet@altanalaw.com**
Jean-Guy de Ruffray / **jgderuffray@altanalaw.com**
Camille Raclet / **craclet@altanalaw.com**