ALTANA
VOCATS • PARIS

EU LAW ON CYBERSECURITY MOVES TOWARDS HARMONIZATION

The EU's implementation in May 2018 of the GDPR and the NIS Directive will constitute a harmonized approach to cybersecurity regulation unprecedented on the old continent. What do companies need to know and prepare in the next 9 months?

LAETITIA DAAGE
ALTANA

JEAN-GUY DE RUFFRAY
ALTANA

On 14 April 2016, the European Union (the "EU") adopted a new Regulation 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, the "**GDPR**"), applicable as of 25 May 2018. It applies to any company collecting or using personal data, regardless of its size.

In addition to the GDPR, the Network and Information Security Directive of 6 July 2016 (the "**NIS Directive**") introduces strict data security and breach disclosure obligations and goes into effect on 9 May 2018.

This set of new regulations, once implemented in the 28 countries of the EU (including likely the UK despite the Brexit), will constitute a common ground of rules applicable to cybersecurity unprecedented on the old continent.

WHAT IS THE GDPR ?

Under the precedent regime of data protection within the EU, each Member State interpreted the EU Directive and enacted its proper laws (example: In France, the "Loi Informatique et Libertés" (French Data Protection Act)), that led to a patchwork of data protection laws and uncertainty for companies' businesses in the EU. On the contrary, the GDPR is directly applicable in all EU member states without the need of national implementation legislation.

In a few words, the GDPR (i) regulates the progression of personal data within the EU, (ii) harmonizes data protection laws in the EU Member states, (iii) eliminates the uncertainty created by a patchwork of data protection laws and (iv) assures European citizens that their data is protected.

The GDPR provides local Data Protection Authorities (DPA) considerable powers to pronounce financial penalties, which can amount to EUR 20 million or 4% of the company's annual worldwide turnover in the event of a breach of basic processing or international data transfer principles, or any requirement of existing EU legislation, depending on: the nature and duration of the infringement and the nature of the data processing; if the breach was committed intentionally or through negligence; if the DPA was notified of the breach and, finally, satisfactory cooperation with the DPA.

Apart from the penalties incurred, there is also a considerable stake in terms of reputation and competitiveness.

A WIDER TERRITORIAL SCOPE OF EU LAW OBLIGATIONS

The GDPR will be applicable:

- to data controllers or processors established in the EU and processing data in the context of the activities of their establishment, whether or not the processing takes place in the EU, and
- regardless of the pace of establishment, to data controllers or processors processing personal data of data subjects who are in the EU for (a) the offering of goods or services to them, or (b) the monitoring of their behavior taking place within the EU.

BURDENSOME NEW CONSTRAINTS ON DATA CONTROLLERS

Under GDPR, data controllers and processors must implement internal procedures and technical mechanisms to prove the establishment of appropriate standards and policies throughout their business. This involves revising the current policy and procedures, which means monitoring, reviewing and assessing the data processing procedures, and building safeguards for all data processing activities.

Under the new "Privacy by design" principle, 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.) For example (i) pseudonymising the data as soon as possible; (ii) guaranteeing transparency; (iii) allowing the data subject to control the data processing.

Under the "Privacy by default" principle, these measures must also comply with the principle of protection of personal data by default in order to guarantee that only the data necessary for each purpose is processed and to allow the user the possibility to expand the privacy parameters thereafter.

These principles are closely linked to the new principle of "accountability", which will lead data controllers to gather relevant documentation likely to demonstrate that data processing is performed in accordance with GDPR, and review and update the related measures taken where necessary.

Lastly, among other essential provisions of the GDPR, the consent of the data subject is now a prerequisite for most of the data processing.

DATA BREACH NOTIFICATION RULES

The GDPR includes a personal data breach notification rule. In case of any personal data breach, (except breaches unlikely to result in any risk to individuals' rights and freedoms), the data controller shall notify the relevant authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If the security breach is also likely to result in a high privacy risk for individuals, these individuals shall also be informed of such breach.

The NIS Directive provides rules about the types of companies, who, in addition to complying with the GDPR, must take measures to protect the security of their network, in their own and general interest. Its measures apply (i) to operators of essential services ("OESs") and (ii) to digital service providers ("DSPs") that are established in the EU or offer services to persons within the EU (in the case of DSPs).

OESs include providers in the areas of energy, transportation, banking, financial market infrastructure, healthcare, drinking water and digital infrastructure services, which are identified as OESs by the Member State in which they are established. DSPs include providers of online market places, online search engines and cloud computing services.

Once the relevant authority has been notified, it may inform the authorities in other affected Member States of the security incident. It may also inform the public, or encourage the company to do so.

It is the responsibility of the 28 Member States to implement the NIS Directive, including identifying the OESs and defining related penalties. In France, the "*Loi de Programmation militaire*" has already partially anticipated the NIS Directive.

Some issues still need to be clarified; for example, there is still uncertainty on how notification under the GDPR and notification under the NIS Directive, once implemented, will have to be executed.

WHAT COMPANIES SHOULD DO NOW TO COMPLY IN LESS THAN ONE YEAR

In less than a year, the GDPR will be fully enforceable and the NIS Directive should be implemented in all Member States. All companies should determine whether the GDPR and the NIS Directive will be applicable to all or part of its activities, and move towards compliance before 25 May 2018. The major steps that should be taken may be summarized as follows:

- Determining whether they are subject to the GDPR and the NIS Directive;
- Inventory and mapping of processing and declarations already carried out by the company, including cross-border transfers of data (The documentation needs to be available to the DPA upon request);
- Determining how the information of the persons concerned and the possibility of exercising their new rights will be implemented;
- Setting up appropriate governance mechanisms;
- Defining the data protection systems by design and by default (pseudonymisation and minimization of data);
- Determining the necessity of nominating a Data Protection Officer (DPO);
- Training and communication plan for company employees;
- Compliance of existing contracts with subcontractors and employment contracts;
- Procedures to be set up to identify security incidents and organize reporting;
- Privacy impact assessment (PIA) when necessary (profiling, sensitive data).

ALTANA

Altana is a full-service business law firm with 80 la1wyers, offering tailor-made legal assistance in complex cross-border and domestic transactions and litigation.

Thanks to its three-fold competencies in criminal law, information technology law and social law, our Cybercrime – Cybersecurity team ensures that their clients are provided with tailor-made, strategic advice and defense, adapted to the technical requirements of each matter.

AUTHORS

Laetitia Daage
Counsel
lddage@altanalaw.com

Jean-Guy de Ruffray
Counsel
jgderuffray@altanalaw.com

www.altanalaw.com