DE GAULLE FLEURANCE & ASSOCIÉS

SOCIÉTÉ D'AVOCATS

Data protection and cyber security

How to improve while securing information technology engineering?

Abstract—*Systems engineering are facing tremendous challenges: on the one hand, more and more sectors deal with high level technologies on a daily basis (artificial intelligence (AI), Internet of Things (IoT), robots and autonomous car), technologies that notably enable a certain level of freedom of the flow of data. On the other hand, all systems need to comply with growing regulations and address increasing cyber security issues.*

The European Union has indeed set up a framework of regulations, notably the GDPR and the NIS Directive, to ensure the protection of users.

This new legal framework can be challenging for international companies with subsidiaries and offices in France or in the European Union but it should not be seen as a hindrance to the business development.

In order to benefit from this amazing technological dynamic, system engineering will then have to use these legal constraints in order to found further opportunities.

Keywords—data protection, cyber security, regulations, liability.

I. OVERVIEW

Data breaches have become one of the most prevalent cyber security incidents around the globe, and it seems the trend is going to continue. In 2017 alone, InterContinental hotels group, Dun & Bradstreet, America's joblink, Verizon Communications, Equifax, Yahoo, Uber or yet TIO Networks are among the most notable incidents. The list for 2018 has begun as early as January with the revelations concerning Carphone Warehouse and US Homeland Security.

Within a context of permanent innovation, where Big Data plays the role of a fuel and new developments such as artificial intelligence (**"AI"**), Internet of Things (**"IoT"**), robots or autonomous cars are our present, or at least our future, businesses need to be aware of their legal and regulatory obligations and potential liabilities. On this point, the European Union has intended to enhance while regulating its 'digital' single market and impose specific constraints for data protection and cyber security. Therefore, engineers and companies need to integrate the issue of compliance from the beginning of all their process and through the whole life cycle of a product or service. This situation, if it may seem burdensome, must be seized as an opportunity to build customers/public trust.

Firstly, the European Union has decided to update its personal data regulation (Directive 95/46/CE) by adopting the General Data Protection Regulation (the "**GDPR**" [1]). This new regulation strengthens controllers' and processors' liabilities while enhancing data subject's rights. It is particularly important for providers of AI, IoT or other new technologies that can use a lot of data including personal data.

Secondly, the protection of users' equipment and/or IT systems more generally (regardless of the issue of personal data) has been increased by the adoption of Directive on security of network and information systems (the "**NIS Directive**"). [2]

This new piece of law requires from providers to implement some strong measures to protect their information system against a risk of security failure or attack.

Consequently, IT engineering needs to comply with the new European law on personal data protection (**1**), as well as on cyber security (**2**). Such compliance is required to avoid legal liability that can be harmful (**3**). This paper

aims to present a global overview to stakeholders in order to help them become familiar with this new framework.

II. GDPR: A NEW FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA IN A DIGITAL TRANSFORMATION ECONOMY

The GDPR will become enforceable as from **May 25, 2018** after a two-year transition period and will be **directly** applicable in all Member States but will also impact **third-party countries** in many situations[1].

The GDPR is set to bring significant changes to the way companies process personal data and introduces a shift in paradigm about compliance. The legislation is designed to **"harmonise"** data privacy laws across Europe[2] as well as giving greater protection and rights to data subjects. Besides, the GDPR no longer requires the completion of most administrative formalities, which shall be replaced by a requirement to implement a series of actions and measures to ensure data governance. Indeed, stakeholders have to adopt a risk and control self-assessment approach towards their 'data capital'. Therefore, controllers and processors are required to be proactive and able to demonstrate their compliance in application of the new **"accountability principle".** The GDPR also fundamentally changes the balance of obligations and liabilities between controllers and processors that are from now on directly liable towards data subjects.

Among their new obligations, data controllers and processors have to implement **Privacy by Design and Privacy by Default** in any project that includes data processing activities [3] . Organizations thus need to consider **privacy** at the initial **design** stages and throughout the complete development process of new products, processes or services ("Privacy by design") and that the default settings should be the most privacy friendly ones ("Privacy by default").

Other obligations can be similar to those under the former framework (such as **lawfulness, fairness and transparency** but also **purpose and storage limitation**[4]) or newer (e.g. **data minimisation** which implies that personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*[5]).

This can also be observed for data subjects' rights with long-time rights such as the right of access but also new ones as it can be illustrated with the right of **"data portability"** which, in some circumstances, give data subject the right to **receive** their personal data, which he or she **has provided** to a controller, in a structured, commonly used and machine-readable format as well as the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided[6]. This new controllers' obligation shall be taken into account when designing new systems (a similar right could be introduced for non-personal data in the future "Free flow of data" regulation [3]). Such a right could raise many issues for stakeholders starting from standardization and interoperability.

More broadly, in a context where data subjects are increasingly concerned about **their** personal **data,** their rights are reinforced, starting with the information about data processing activities that they are entitled to receive from data controllers and/or processors which is extended. But data subjects can also, for example, object or limit the processing of their data (with a direct right of action against profiling and/or automated individual decision-making)[7] or exercise their right to be forgotten (then data controllers have to delete their personal data)[8]. It all boils down to trying **to empower individuals facing the massive exploitation of their data** (an objective also pursued by the new **e-privacy regulation** which is still under negotiations [4]).

As it can be perceived through this first glimpse, **the GDPR brings many challenges for organizations to comply with**. This is why most of them have started to question their practice and launched compliance plans.
The first step to achieve this goal is to conduct a **data mapping** and to organize the project **governance**. For some organizations, a **Data Protection Officer ("DPO")** will be appointed (whether by choice or because they are compelled to do it by the GDPR[9]).

When performing this task, it is important to bear in mind that **'personal data'** is broadly defined, as it can be direct or indirect identifying information. It can also be structured or unstructured data (e.g. e-mail inbox). Data reconciliation shall receive a special treatment. IoT business should also be particularly cautious about the processing of **sensitive data** such as those relating to data subjects' health that receive a special treatment under the GDPR (e.g. when developing connecting bracelet or scale). Thanks to this mapping, an **action plan** can be built and implemented over time.

[1] Indeed, a business established outside the European Union will notably be subject to the GDPR if it targets individuals in the EU. Even if this is not the case, it will have compliance obligations if it is processing data on behalf of a company that is covered by GDPR.
[2] Nonetheless, some provisions give a **margin** of appreciation to **Member States** if they wish to intervene.
[3] Art. 25, GDPR.
[4] Art. 5, GDPR.
[5] Art. 5, GDPR.
[6] Art. 20, GDPR.
[7] Art. 21 and 22, GDPR.
[8] Art. 17, GDPR.
[9] Art. 37, GDPR.

9, rue Boissy d'Anglas - 75008 Paris - France - Phone: + 33 (0)1 56 64 00 00 / 222, avenue Louise - 1050 Brussels - Belgium - Phone: + 32 (0)2 644 01 64

The GDPR is a **transversal project** that requires mobilizing numerous resources and skills within an organization. A wide range of functions are involved, and not only **the Legal and IT Department** (even if these two departments do have the leadership). In this respect, all business units such as Human Resources have to be involved (especially as lots of data leaks are caused by an action or failure of someone in the company). **Staff** must be well informed and thoroughly trained if an organisation is to prevent sensitive data being accidentally or deliberately compromised.

The GDPR's obligation to implement appropriate technical and organisational measures will also help companies building their cyber security policy.

III. NIS DIRECTIVE: IMPROVE CYBERSECURITY IN ORDER TO ENSURE USER'S CONFIDENCE

In order to achieve cyber security, an information system shall be able to prevent cyberspace events that may compromise the availability, integrity, or confidentiality of stored, processed, or transmitted data, and related services either provided by these systems or accessed through them[10]. This has become a major issue, as about 80% of companies have already suffered from a cyber-attack[11].

European Union also counts it as a crucial issue, therefore on July 6, 2016, the Parliament and the Council adopted the NIS Directive. This Directive, that has to be implemented by each EU Member State on **May 9, 2018 at the latest**[12], applies to operators of essential services ("**OES**"), i.e. a public or private entity that intervenes in specific sectors including energy, health or transportation sectors, and digital services providers such as an online marketplace, search engines or cloud computing services. However, it does not apply to micro and small enterprises representing less than 50 persons or whose annual turnover or total annual balance sheet is less than 10 million euros[13]. **Member State may expend the scope of the implemented Directive to other actors.**

The aim is to protect networks and information systems, whether they involve personal data treatments or not, against cyber risks and incidents and **the failing company may face heavy fines** should it fail to comply with the relevant regulations.

The Directive notably lays down an obligation for digital service providers and OES to **identify security risks** and then to **set up technical and organizational measures** against these risks. These measures have to be appropriate and proportionate to the risks. The level of security must be adapted to the existing risk taking into account security of systems and installations, incident management, business continuity management, monitoring, audit, control, compliance with international standards. Furthermore, services providers, as operators of critical infrastructures, shall **report such incidents to the relevant authority**[14], take steps to avoid and limit the impact of security incidents to ensure continuity of essential services or digital services such as online marketplace, online search engine and cloud computing service.

In order to fulfil their obligations under the NIS Directive and ensure effective cyber resilience, IT service providers need to implement **best practices**. Firstly, they need to set up **technical tools** enabling the detection of any breach in the system and strengthening information system such as encrypted data. Secondly, because the main source of cyber risks is human, the company at stake shall **implement intern standards and policies** relying on regular security audits. This audit will be the basis of the information security charter that will be annexed to the internal employees regulations. The DPO, in cooperation with the human resources department, will ensure that the aforementioned charter will be fully respected. Finally, as provided for by the GDPR, it is highly recommended to create and maintain a register of risks and infringements.

Therefore, the collection of personal data by IT engineering shall comply with the GDPR requirements and the information system of an IT service provider shall be protected against cyber-attacks as provided for by the NIS Directive. **Compliance with these regulations is a mandatory condition to be fulfilled in order to deny one's liability should any harmful event occurs.**

IV. COMPLIANCE TO DRIVE OUT LEGAL LIABILITY

All these new regulations regarding data and information systems and how they should be secured have to be put into perspective with the current development of new technological devices, such as the IoT, drones, robots or autonomous cars. These devices will process tremendous quantities of data, often directly collected from end-users and as such represent a security weakness. Therefore, such devices may trigger **potential dual liability for the providers**. The first liability is based on the violation of the data itself. The second may be - in the near future - the liability regarding the damage made by the object to its environment.

Regarding the importance of the GDPR regulation and the risk attached thereof, stakeholders' compliance with this regulation is a crucial issue notably because of the **administrative penalties than can from now on reach up to 20 million euros or 4% of the previous year's annual worldwide turnover** (whichever is higher). This is only the tip of the iceberg that must not let organizations forget other negative consequences (e.g. damage to the company's image, potential class-action from data subjects or obligation to stop processing activities). Several examples in France highlighted by the

[10] Definition from security of information system french agency.
[11] Annual survey cesin opinionway 2018 - Business Cybersecurity.
[12] It has been implemented in France on February 15, 2018.
[13] Within the meaning of Recommendation 2003/361 /EC.
[14] In France, the ANSSI ("*Agence nationale de la sécurité des systèmes d'information*").

French data protection authority (CNIL) are a clear reminder of the potential risks arising from connected toys or cars.

Besides data breaches, damage may arise from the device itself when it interacts with the real world. That is the case for robots or autonomous cars for example. In this perspective, cyber security is very important to avoid any act of hacking against such devices.

Even without illegal hacking, one may think on a wider scale about the liability issue of the owner, the user or the creator of the device, or also of the software developer that **may be subject to a direct liability**.

The ground of such legal prospective is the European Directive on product liability [5], which could be modified in order to adapt it to technological developments and issues arising from this new trend. Such directive provides that the producer shall be liable for any damage caused by a defect in its product if it does not provide the safety that a person is entitled to expect. Such safety would probably in the future be analysed by taking into account the cyber safety, putting more pressure on product manufacturer. Indeed, this has an impact on software editors that provide their software as a component of the device, since they may be jointly and severally liable with the manufacturer of a finished product in which the software is integrated. It also strongly impacts the insurance business and coverage.

All these issues need to come under scrutiny and to be well anticipated. In this perspective, the GDPR and the cyber security regulation should be seen as opportunities for any company wishing to deploy itself into the next generation of devices.

CONCLUSION

Understanding the impacts and challenges of data protection and cyber security for information systems regulations is critical for IT engineers and software developers.

However, the multiplicity of legal and regulatory sources (the GDPR, the NIS directive, international standards, national legislations…) is a complicating factor. It makes it more difficult for stakeholders to have a clear picture of their obligations as the liabilities they may now face.

Supervisory authorities and soft-law bodies will have an important role to play from this point of view in providing further clarity.

REFERENCES

[1] Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[2] Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Proposal for a regulation on a framework for the free flow of non-personal data in the European Union, September 13, 2017.

[4] Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, January 10, 2017.

[5] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

Content as of April 30, 2018.

Contacts:
Béatrice Fleuris, Partner, +33 1 56 64 16 55, bfleuris@dgfla.com
Georgie Courtois, Partner, +33 1 56 64 16 52, gcourtois@dgfla.com
Nina Gosse, Attorney, +33 1 56 64 17 21, ngosse@dgfla.com