**Distribution / Competition / Consumer – Information Technologies Update**
*May 2017*

SHARE

# Designers and operators of connected devices: Beware the new personal data protection rules!

The number of connected devices is expected to reach 50 billion by 2020. The development of the Internet of things (IoT) not only represents a worldwide market worth billions of dollars but also an opportunity for many companies to change business models and switch from selling goods to selling services. However, operating a connected device implies keeping control of the data throughout, when they are being collected, analysed, and then put to use. Therefore, data are the sinews of connected devices and the source of two major concerns for users and two major challenges for creators: the use of data other than for the purposes of the connected device (and especially for marketing or advertising purposes) and data security breaches.

EU regulation no. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (the General Data Protection Regulation, or GDPR) lays increased responsibility on those who design and organise the processing of data ("controllers"). This complex and technical piece of legislation (173 whereas and 99 articles) is about to bring about profound changes to the practices, documentation and organization of businesses who will have to integrate greater data protection from the design stage.

## Scope

The regulation, which is due to **come into force on 25 May 2018**, will apply directly not only to **businesses established within the European Union**, irrespective of where the data are being processed, but also to **businesses established without the European Union**, provided they sell goods or services to "data subjects" within the EU or follow the behaviour of persons established within the EU. The GDPR applies to **any processing of personal data** (PD) whose definition has been significantly increased to cover the identification of any physical person by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to their genetic, mental, economic, or other identity.

Even though the French Data Protection Act no. 78-17 of 06 January 1978 (recently supplemented by the French Digital Republic Act no. 2016/1321 of 07 October 2016) already lays many obligations on PD controllers and grants rights to data subjects, economic operators designing and commercialising or operating connected devices or commercial web sites or applications must start getting ready for the GDPR now.

## Personal data protection by design and by default

Under the new rules, manufacturers of connected devices must integrate PD protection at the design stage in accordance with two major principles: data protection by design and data protection by default. **Protection by design**: When determining the means for PD processing, controllers must implement appropriate technical (software and hardware) and organisational (training, process, control, etc.) measures in order to make sure PD processing complies with the GDPR's general principles. **Protection by default**: When designing the architecture of (e.g.) a connected device, controllers must ensure the device by default only collects and processes such personal data as required for the purpose of the processing. In other words, PD protection is no longer a purely legal issue to be examined once the digital tool has been built.

The GDPR provides that all data processing must be lawful, fair, and transparent. Personal data may only be collected for specific, explicit, and lawful purposes and the collected data must be adequate, limited, correct, up-to-date, and stored only for a limited period of time.

The same idea is behind the requirement for a **data protection impact assessment** (DPIA). Where PD processing operations *"are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes"*, a DPIA must be carried out before processing can begin. All businesses, irrespective of their size, that distribute or plan to distribute connected devices must carry out such an assessment where the risk to the rights and freedoms of natural persons is high. The DPIA must in particular include an analysis of the adequacy between the purpose of the processing and the type of collected

data as well as an assessment of the risks to the rights and freedoms of data subjects and of the technical security measures required in order to guarantee the protection of the data.

### Greater protection

The GDPR goes beyond the rights currently enjoyed in France under the French Data Protection Act in that **it grants data subjects several additional rights**: in addition to the rights of access to and rectification of data, data subjects now have a right of erasure, a right to restriction of processing, a right to data portability, and a right to object to processing. Data subjects must be explicitly advised of all these rights, which must be effectively implemented by the controller at the data subject's request. Correlatively, **the information to be provided** to data subjects (users of connected devices) has been fleshed out (the regulation includes a dozen clearly listed items) and must be easily accessible and expressed in clear language. These various rights and this exhaustive information are therefore going to have an impact not only on the contents of confidentiality notices but also on the way interfaces associated with connected devices are displayed.

Lastly – and this is not the least of the GDPR's contributions – **the validity of the data subject's consent** is more strictly regulated insofar as such consent must be specific, informed, unambiguous, and freely and actively given by the data subject and recorded by the controller. Here again, the strengthened conditions for expressing consent will have an influence on the design of connected devices.

### Greater accountability

As from May 2018, the current French notification system will lapse in favour of a system that will give controllers a far greater sense of responsibility in that they will be personally responsible for implementing procedures and means intended not only to comply with all the obligations provided for by the GDPR but also to prove compliance therewith (the so-called "accountability" principle).

Controllers must therefore create and scrupulously maintain **records of processing activities** which may be audited at any time by the French data protection agency (CNIL). All controllers are concerned, including PD processors (e.g., businesses leasing servers), regardless of the purpose of the PD processing. However, companies with less than 250 employees do not have to keep records of processing activities unless any one of the three following criteria is met: processing is likely to result in a risk to the rights and freedoms of natural persons, processing is not occasional, processing concerns sensitive data categories (e.g., health data).

Likewise, the GDPR provides that a **data protection officer** (DPO) must be appointed where *"the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale"*. The DPO may be either an employee or a service provider and their task will be central to the company because, in addition to ensuring that the controller complies with their obligations under the GDPR, the DPO will inform and advise them on any required measures, will help raise awareness to compliance with PD protection rules, both internally and externally, and will cooperate with the CNIL. In time, the practice of appointing a DPO will probably spread to businesses whose processing activities do not necessarily require one.

### Greater security

Another of the GDPR's principles is that the controller must **ensure an appropriate level of security** against unauthorised processing, loss or destruction of personal data. Under the GDPR, controllers must take all technical measures to ensure increased computer security. Opinion surveys show that the major obstacle to the development of connected devices is the users' fear that their personal data might be stolen. What is striking here is the gap between, on the one hand, natural persons' (probably exaggerated) perception of the hijacking/piracy risk to their data, and on the other hand, the oblivion of connected device designers who apparently continue to underestimate the risk and fail to take appropriate measures, e.g., by pseudonymizing, anonymizing, and encrypting data exchanges, forcing users to choose complex passwords, or offering secure web interfaces.

The corollary of the security principle is the **notification obligation for controllers and processors in case of PD breach**. Actually, controllers have a **double notification obligation** (subject to conditions and of a varying nature, depending on whether the breach is likely to result in a "high risk" to the rights of persons or not), towards the supervisory authority (the national data protection agency, here the CNIL) on the one hand, and towards the data subjects concerned by the security breach on the other hand. Furthermore, under the GDPR, controllers have a duty to document any PD breach (irrespective of its seriousness) in a **register of incidents** which may be audited at any time by the supervisory authority.

### Liability

With the GDPR, the risks incurred by connected device designers and operators are particularly high and varied.

The first risk is a **civil liability** risk: Controllers may be held liable, jointly and severally with joint controllers or with processors, as the case may be, if they fail to faultlessly process or secure personal data. Agreements between such parties should therefore clearly pass on obligations under the GDPR and should for example provide for audit or rectification procedures for the benefit of the controller.

Secondly, the GDPR authorises national authorities to impose **administrative fines** that are nothing like currently available penalties. The fines, which the GDPR recalls must be effective, proportionate, and dissuasive, can reach 10 million euros and 2 % of turnover or, in some cases, 20 million euros and 4 % of turnover, depending on the gravity of the breach. Therefore, a breach of PD protection rules may potentially threaten a business's entire financial equilibrium.

Thirdly, controllers who fail to comply with the GDPR's rules will incur a response from competitors (possibly in the form of an **unfair competition action** on the grounds of non-compliance with administrative regulations) but first and foremost from users/consumers who will probably be entitled to initiate a class action. However, the most effective – albeit indirect – sanction will surely come from **certification body rankings** which the GDPR openly encourages to commercially punish connected device designers who fail to comply with PD protection rules.

Designers and operators of connected devices that require PD processing therefore need to take into account both these "hard" penalties and this "soft law" in order to turn the protection of personal data into a competitive edge rather than view it as a legal or computing constraint. They have 12 months.

By Christophe Héry

---

**Contact: Christophe Héry**

LmtAvocats

E-mail: chery@lmtavocats.com

www.lmtavocats.com

Tel.: +33 1 53 81 53 00

Fax: +33 1 53 81 53 30

**Follow us on**

**Click here to view our previous Distribution Updates on :**

- Restrictive business practices and price transparency
- Significant imbalance and freedom to negotiate prices
- Sudden termination of international commercial relationship
- Private enforcement and new rules in France

**Click here to view all Lmt Avocats previous Updates : Lmt Avocats Newsletters**