

Personal Data: What can you expect?

Posted on Monday 24th of October 2016 in Employment, Pensions & Immigration, IP, IT & Media

Following the recent adoption of the EU data protection reform, companies handling personal data will need to focus on their privacy policies and internal practices to ensure they meet the high new reformed standards. In this context, it is crucial to draw the line between personal data to which data protection rules apply and simple information. Here is some advice to help you to make this distinction.

Broad definition of personal data

Under EU[1] and Luxembourg Law[2], “personal data” means **any information of any type relating to an identified or identifiable natural person, regardless of the type of medium:**

- “Any information” covers **objective** (e.g. blood type) as well as **subjective** (e.g. opinions, assessments) information related not only to the private life of individuals, but also to their public and professional life.
- **Data relates to an individual** where it concerns his/her i) identity, ii) characteristics, iii) behaviour, or has an impact on the way the individual is treated or evaluated. Information relating to objects which can be used to identify a person also constitutes personal data (e.g. vehicle licence plate number used to establish a link between the car and the owner, Ip addresses enabling the identification of a computer and so of its owner).
- A person is **identified** if his/her identity is manifestly obvious (e.g. a person designated by first name and surname) and **identifiable** if his/her identity can be established by using additional information, such as i) identification number, ii) physical, physiological, mental, economic, cultural, social characteristics (e.g. gender) or iii) a combination of criteria such as age, place of residence, occupation, etc.

Data protection rules are designed to protect only natural persons, regard-less of their quality (employees, website users, suppliers, etc.)

- Personal data can be stored on **any type of medium** such as paper, computer memory, DVDs, USB sticks, etc, and presented in **any format** (alphabetical, numerical, graphical, photographic, acoustic, etc.)

However, data protection rules do not apply to processing i) in manual non-structured form or ii) undertaken for purely personal or household activities by a natural person.

Anonymisation v. Pseudonymisation

- **Anonymised data** refers to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the individual is not or is no longer identifiable. **Data protection rules do not apply** to this type of information, **as it does not contain any identifiers.**

- **Pseudonymised data** refers to personal data that can no longer be attributed to a specific data subject **without** the use of additional information, which is kept separately. These data contain **encrypted identifiers** and **therefore fall under the scope of data protection rules**.

Examples of personal data

A large number of economic players (either private or public) can face personal data issues in their daily business, either in relation to their clients (e.g. client lists), suppliers, or in relation to their employees (e.g. corporate emails, pay slips), across all industries.

- **Financial industry** deals with a variety of specific personal data such as bank account information, transaction details, customer's instructions where they are recorded, information relating to the creditworthiness of borrowers and loan applications. Financial institutions must pay special attention to compliance with data protection rules when undertaking Anti-Money Laundering procedures, which could reveal sensitive information (link to terrorist organisations, criminal convictions, etc.)
- **Retail industry**, such as supermarkets, makes use of personal data when building consumer profiles or implementing promotional programs or sweepstakes.
- **Health sector**: medical history, test results, diagnosis, drug prescription information, etc., amount to sensitive personal data about the patients (see below).
- **In an employment context**, employers must comply with data protection rules. This starts from the hiring process of employees and continues during the performance of the contract (also where they use video surveillance, geolocalization systems or log files). It also extends after the end of the employment relationship.
- **In general**, use of **new technologies** generates large amounts of personal data such as IP addresses, cookies, emails, content published or transmitted via social networks.

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life (i.e. "sensitive data"), is subject to a restricted regime.

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 2 (a).

[2] Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, as modified, Article 2 (e).

We would be happy to help you to assess whether your processing activities involve personal data and therefore require compliance action.

Please contact us for more information.

[Download this news in French](#)

Your contact(s)



Virginie LIEBERMANN

Senior Associate

Avocat à la Cour, Member of Luxembourg Bar, 2008

virginie.liebermann@molitorlegal.lu