PDG Avocats

French Data protection topics of interest for the Life Sciences Industry

Data protection issues: exciting issues for specialists but boring and frightening problems for many people within industry. Based on our experience and on recent files, please find below a few situations which may require your attention.

Personal data is defined under French law as any information relating to an identified or identifiable individual. An individual is identifiable when he can be identified, directly or indirectly, for example by an identification number such as his social security number or by indications relating, for example, to his name and first name, date of birth, biometrics data, fingerprints, DNA…

Such personal data is regularly collected and processed by Life Sciences companies within the framework of their activities such as clinical trial **(1.)** or compliance activities **(2.)** and in parallel transferred outside the European Union to the parent company located for example in the United States (US) **(3.).** Data protection issues may also appear within the framework of discovery procedures taking place in the US and involving French data **(4.)** Other issues may also be of interest **(5).**

1. Clinical trials

The French Data Protection Commission (CNIL) drafted a Reference Methodology (MR-001) modified in October 2010 on the processing of personal data in clinical trials.

If the requirements provided in the Reference Methodology are fulfilled, companies may only provide the CNIL with declaration of conformity. The companies will consequently avoid the long procedure of authorization with the CNIL which is constitutes of:

- Firstly, a request of opinion of the Consultative Committee for the Processing of Information relating to Research in Health Matters (CCTIRS). After a one-month period, the silence of the CCTIRS is considered as a favourable opinion.
- Secondly, a request of authorization of the CNIL.

The Reference Methodology applies to clinical trials for medicinal products and medical devices but does not cover clinical trials in which the complete identity of the patient is available or to genetic researches which identify the genetic characteristics of the patients.

The following data can be collected:

- Identity: it must be an identification number or an alphanumeric code;
- Health: the therapy followed, examination results, diseases, etc;
- Signing information: age, date of birth, sex, weight, size;
- Date of inclusion;
- Ethnical origins if relevant for the trial;
- Genetic variations in response to a medicinal product or device, if relevant for the trial;
- Family situation;

- Economic and financial situation;
- Tobacco, alcohol, drug consumption;
- Life habits;
- Dependence;
- Assistance
- Physical exercise;
- Way of living;
- Sexual life if relevant of the trial
- Validated quality of life scale.

The Reference Methodology indicates furthermore that the personal data collected must be obtained from the patient himself and the investigators. The category of persons authorized to implement the processing and the one authorized to have access to the data are defined in the Reference Methodology.

The Reference Methodology also reminds of the obligation of information of the patients on the processing of personal data and the need to obtain the specific authorization of the patient in case of collection and processing of genetic data.

2. Compliance: Assessment of whistle-blowing systems

The CNIL acknowledges that the whistle-blowing system is mandatory for listed companies in the US under the Sarbanes-Oxley Act. It appears according to the observations of the CNIL that these whistle-blowing systems which are set up by US parent companies seem unsuitable to the usual practices of French companies.

Furthermore, according to the CNIL, the legal requirements of the the French Data Protection Act (Law No. 78-17 of 6 January 1978) for the implementation of whistle-blowing systems are not always understood. Indeed, the whistle-blowing system is often linked to the company's code of conduct, which scope does not always comply with what is allowed by the CNIL.

The CNIL has adopted a Unique Authorization (AU-004) on 8 December 2005 modified on 14 October 2010 to give a framework to the implementation of whistle-blowing systems and simplify administrative formalities with the CNIL. The companies that comply with the defined framework must only provide the CNIL with a declaration of conformity. If the whistle-blowing system set up by the company does not comply with the framework of the Unique Authorization, the company must file a complete authorization dossier with the CNIL.

To benefit of the Unique Authorization the companies must in particular comply with the following rules:

- The whistle-blowing system must be **optional**. The employee cannot be sanctioned by the company if he does not declare a failure.

- The whistle-blowing system must only be used to obtain declarations of **severe accounting, financial facts or relate to corruption or to competition law.** If a

misbehaviour that does not fall within this scope is declared, the person must be oriented to the appropriate department within the company (for HR or finance).

- **The declaration of misbehaviour shall not be made on an anonymous basis**. To avoid any risks of slips and to protect to author of the declaration, the person shall be invite to give his identity.

- The employees must in particular be **clearly and previously informed** of (i) who is responsible of the system, (ii) the scope and purpose of the whistle-blowing system in place, (iii) the optional character of the declaration and the absence of sanction in case of no declaration, (iv) the recipients of the declarations and (v) their rights of access and rectification.

- The processing of the declarations must be treated by a **dedicated department** or organism. The persons in charge must be specifically trained and bound to a confidentiality obligation.

3. Transfer of Data outside the European Union (EU)

Every year, the CNIL authorized a large number of transfers outside of the EU. Data flows may be transferred at the request of the parent company located for instance in the US for management reasons.

The transfer of data outside of the EU needs an authorization to be filed with the CNIL. The authorization file will have to include warranties on the protection of the data such as an agreement between the data controller and the data recipient on the transfer, Binding Corporate Rules or joining the EU-US Safe Harbor program. The CNIL will delimit the scope of the transfer. Details on the transfer will have to be given in the authorization file.

Employees must be previously informed of the transfer of data. This information must be drafted in French. A template of information sheet is available on the CNIL website (www.cnil.fr)

The CNIL has a 2-month-period (renewable once) to give its answer. At the expiration of this period, the silence of the CNIL is considered as an authorization.

A complete lack of compliance with the legal obligations of the French Data Protection Act constitutes an offense punishable by 5 years in jail and a €300,000 fine in pursuance of Article 226-16 of the Criminal Code.

4. Discovery

The transfer of data within the framework of a discovery procedure is covered by the exception of Article 69-3 of French Data Protection Act according to which "*the data controller may transfer personal data to a State not satisfying the conditions provided for in Article 68 if the data subject has expressly consented to their transfer or if the transfer is necessary subject to one*

of the following conditions for: (…) 3° the meeting of obligations ensuring the establishment, exercise or defence of legal claims".

According to Deliberation No. 2009-474 dated 23 July 2009 on discovery procedures, no formalities are requested by the CNIL but the CNIL specifies that the transfer must be unique and not be massive. If the transfer is considered as massive, an authorization of transfer as described in 3. will be necessary.

5. Other issues of interest

In the health field, the question of anonymisation is essential. The CNIL is very sensitive to how the data is anonymised and will check this aspect when examining an application in this field. So we recommend carefully preparing the anonymisation phase when constituting databases.

As seen above, the CNIL has put in place some methodologies and simplified declarations to ease the procedures of the companies when declaring databases to the CNIL. However, this is not always possible and in some cases such as the constitution of bio-collections, a full authorization dossier will have to be filed.

Moreover, we will like to draw your attention to involuntary interconnection between databases.

Finally, foreign companies should not forget to check internally that necessary formalities regarding the existing databases are in place. All databases created must be declared to the CNIL. The CNIL has established simplified declarations for a number of basic databases usually created in companies. This is the case, for example, for databases of employees (simplified declaration No. 46) and databases of clients (simplified declaration No. 48).

In its annual plan adopted on 24 March 2011, the CNIL indicated an objective of 400 controls in 2011. security of health data still being one of its priorities, you better show, at least, that you are conscious of your lacks if any and on the way to repair them if you are one of those 400 companies which will have a CNIL audit this year.

Paule Drouault-Gardrat and Juliette Peterka
PDG Avocats

(with our thanks to Benoît Louvet with whom we regularly collaborate in this field)

Contact: pdrouaultgardrat@pdgavocats.com