International Bar Association

How to process health personal data under French law after 25 May 2018

Wednesday 5 September 2018

Cécile Théard-Jallu *De Gaulle Fleurance & Associés, Paris*
ctheardjallu@dgfla.com

Nina Gosse *De Gaulle Fleurance & Associés, Paris*
ngosse@dgfla.com

While the European Union's recently enforced General Data Protection Regulation (GDPR) directly applies within EU national laws, Member States still retain the ability to derogate from certain aspects of the regulation. This means that any controller or processor needs to become familiar with the articulation between different sets of legislations at EU and domestic level.

France has seized this opportunity and updated its domestic legal framework accordingly. Here is an overview of the new French legislation with a focus on health data processing.[1]

Symbolically, France decided to maintain its historic Act No 78-17 (LIL) dated 6 January 1978 on information technology, data files and civil liberties while amending it to take into account the entry into application of the GDPR on 25 May 2018.[2] This was done with the enactment of Act No 2018-493 on personal data protection on 20 June 2018. This law also transposed Directive 2016/680 concerning data processing in the areas of judicial cooperation in criminal matters and police cooperation.[3]

Among other issues, the updated LIL introduces substantial changes into the previous French health data-processing framework. This article presents the main features of the new regime to be observed by stakeholders and, more specifically, when it applies and, above all, how to comply with it.

Territorial scope

Without prejudice to the territorial rules of the GDPR, the modified LIL now applies as soon as the data subject resides in France, including when the controller is not established in France (Article 5.1). This criterion has been added to two pre-existing criteria; that is, either the controller is established on the French territory or the controller uses processing facilities located on the French territory (Article 5).

French regime for processing health data

France has always reserved a specific regime for personal health data processing. Indeed, personal data relating to health cannot be processed unless authorised by the LIL. The French specific regime relating to health data now entirely lies in Chapter IX of the LIL as modified.

In order to help stakeholders understand the obligations to be complied with, two scenarios can be distinguished.

As a preliminary remark, French law does not apply to personal data of deceased persons including information that appears on certificates of causes of death. In other words, this data may be processed unless the data subject has, during their lifetime, expressed their refusal in writing that such processing takes place (Article 57 of the LIL). This is in line with Recital 27 of the GDPR, which excludes from its scope the data of deceased people.[4]

First scenario

In the first scenario, the health data processing is exempt from the application of Chapter IX of the LIL.

Article 53 of the LIL as modified provides for a list of exceptions that lift the prohibition to process health personal data:

- first set of exceptions: those described in categories 1 to 6 of Article 8 of the LIL:

  – processing for which the person has given consent;

  – processing necessary for the safety of a human life, while the person cannot give consent;

  – processing carried out by an association or any other non-profit organisation of a religious, philosophical, political or trade union nature (in relation to its purpose and members);

  – processing of personal data made public by the data subject;

  – processing necessary for the establishment, exercise or defence of a legal claim; and

  – processing necessary for the purposes of preventive medicine, medical diagnosis, the administration of care or treatment, or the management of health services and carried out by a member of a health profession, or by another person who, by reason of their duties, is bound by the obligation of professional secrecy;

- processing enabling studies to be carried out on the basis of data collected in the context of preventive medicine, medical diagnosis or the administration of care and treatment, *where such studies are carried out by the healthcare team and intended for their exclusive use*;

- processing intended to ensure the provision of benefits or supervision by the bodies responsible for administering a basic health insurance scheme and the payment of benefits by supplementary health insurance bodies;

- processing carried out within health institutions by doctors responsible for medical information, under the conditions provided for in the second paragraph of Article L. 6113-7 of the French Public Health Code (CSP) (ie, analysis of the activity of the institutions); and

- processing carried out by regional health agencies, by the French State or by the public person it designates (information relating to their means of operation, their activity, their health, demographic and social data that is necessary for the development and revision of the regional health project, the determination of their resources, the evaluation of the quality of care, health monitoring and vigilance, as well as the control of their care activity and their invoicing).

However, in these cases, data subjects have the right to object to the lifting of professional secrecy for data processing (Article 57, LIL).

When personal health data processing falls under one of its exceptions, it will only be subject to the GDPR's provisions and LIL's general obligations and not to the French specific regime relating to the processing of health data subject matter of Chapter IX of the LIL.[5]

Second scenario

In the second scenario, the processing is subject to the French specific regime relating to health data (embodied in Chapter IX of the LIL as modified).

When personal health data processing cannot be grounded on any of the previously mentioned exceptions, it will be subject not only to the GDPR but also to the French specific regime relating to health personal data, which is developed below (Chapter IX).

General obligations for all personal health data processing

Public interest requirement (Article 54.I of the LIL)

The first consequence is that, in such a case, the processing will have to be justified by a *public interest*. Ensuring high standards of quality and safety for healthcare and medicines or medical devices is expressly mentioned as an example of a purpose representing a public interest.

This notion is different from the notion of 'public interest' mentioned in Article 6.1.e of the GDPR[6] (ie, one of the legal bases for data processing) as it more specifically refers to a mission conferred by law or by a public authority.

As far as it is concerned, Article 9.2.i of the GDPR is relevant and states that: 'processing is necessary for reasons of public interest in the area of public health, *such as* protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.'

As indicated by the use of the terms 'such as', this list is not exhaustive. Consequently, 'public interest in the domain of public health' may still exist beyond

the illustrations listed in Article 9.2.i of the GDPR but it will then need to be recognised as such by the French Data Protection Authority (CNIL) on a case-by-case basis.

Administrative formalities (Article 54.II and 54.III of the LIL)

If not entering into any of the express exceptions laid down by the LIL as aforementioned, there are two ways to proceed in order to validate a health data processing under French law: either the processing is compliant with pre-defined standards set forth by the CNIL (option 1), in which case the controller will only need to commit to comply with such standards by filing an online declaration with the CNIL; or, if not, the controller will need to submit an ad hoc authorisation application with the CNIL (option 2).

Regarding option 1, the modified LIL invites the CNIL to issue those standards either in the form of standard guidelines (*référentiels*) or standard rules (*réglements type*) on which controllers can rely.

Very few of them already exist under the modified LIL and we will need some more time for this referential content to be developed. This being said, on 13 July 2018,[7] the CNIL started issuing some standard guidelines in the domain of medical research (see dedicated section in this article) with the publication of five new so-called *méthodologies de réference* (MR), covering a variety of interventional or non-interventional research practices on human beings as well as processing requiring an access to the data collected within the new French national health data repository (*Système national des données de santé* – SNDS, which is managed by the French National Institute of Health Data – INDS).

Actors whose processing activities do not fall within the scope of such standard guidelines or rules (option 2) will need to require a prior authorisation from the CNIL. The CNIL will then have two months (renewable once upon a motivated decision of the CNIL's president or if the INDS is consulted) to decide on such an application. In the absence of any reply from the CNIL within this deadline, the authorisation shall be deemed granted unless in relation to health research activities if a negative opinion has been rendered by involved consultative bodies (see section on research projects below).

Confidentiality of health data (Article 56 of the LIL)

In cases where the health professional transmits identifying personal data to an authorised data controller, they both must guarantee that the data is kept confidential. Again, the CNIL is entitled to adopt recommendations or guidelines on the technical processes to be implemented in this respect.

Persons in charge of the data processing and those who have access to the data shall be bound by professional secrecy under the penalties provided for in Article 226-13 of the French Criminal Code.

Specific provisions on research, study or evaluation purposes (Articles 61–64 of the LIL)

These provisions apply to automatic processing of personal data for research or studies in the field of health or the evaluation or analysis of care or prevention practices or activities.

While the system remains the same (reliance and commitment to comply with the CNIL's standard guidelines and if none is available, obligation to obtain the CNIL's prior authorisation as aforementioned), some specific provisions shall also apply, which are summarised below:

- referentials will take the form of MRs – as aforementioned, five new MRs have been published on 13 July 2018;
- authorisation from the CNIL shall be adopted after a preliminary opinion is issued by specific committees (the *Comité de Protection des Personnes* – CPP or *Comité d'Expertise pour les Recherches, les Etudes et les Evaluations* – CEREES) depending on the nature of the research, these committees respectively representing the interests of patients or helping the CNIL validate the methodological and scientific aspects of application files);
- the CNIL may also consult the INDS on the public interest pursued by the research;
- contrary to the general case previously mentioned, the CNIL's tacit authorisation will only be possible if preliminary opinions of those consulted bodies were expressly favourable;
- some specific provisions apply to the information of minors as well as the exercise of their rights;[8] and
- the creation of an audit committee within the aforementioned SNDS.[9]

Specific provisions for processing of genetic data

Under the GDPR, genetic data[10] is considered as sensitive data (Article 9.1) and as such can also be subject to national restrictions.

Under French law, genetic data can be processed: on behalf of the French State acting within the framework of its prerogatives of public authority and as authorised by decree to be adopted by the French Council of State (*décret en Conseil d'Etat*) based on a public and motivated opinion of the CNIL (Article 27 of the LIL); or in the context of health research and with an 'informed and express consent' from data subjects.

Lastly, it should be noted that processing of the social security number (the *Numéro d'inscription au Répertoire* – NIR), which is not considered 'sensitive data' per se, is nonetheless subject to a specific regime under French law. Indeed, such processing must be covered by a decree issued by the French Council of State taken based on a public and motivated opinion of the CNIL (Article 22 of the LIL), except under specific circumstances (eg, processing carried out by the public statistical service for the purpose of producing public statistics and without sensitive data).

Historically, France has had specific and tight rules on the protection of health data. Although it has updated those rules through modifying the LIL to absorb the GDPR's new paradigm and take into account past experiences, French legislation stays in this protective mindset to grant greater security for data subjects as well as trust in the entire ecosystem, which in the end is hoped to trigger economic value for the healthcare sector.

Notes

[1] This article was drafted on 31 July 2018.

[2] However, the French government still needs to adopt an order (*Ordonnance*) aimed at rewriting or somehow 'cleaning' the 1978 Act and bringing into consistency neighbouring texts containing references to it.

[3] European Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[4] Recital 27, GDPR: 'This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.'

[5] Article 55 also excludes from Chapter IX some specific bodies' processing operations implemented to respond, in an emergency situation, to a health alert and to manage the consequences thereof. These operations are only subject to the GDPR provisions on data impact assessments (Chapter IV, Section 3 of the GDPR).

[6] Article 6 of the GDPR ('Lawfulness of processing'): '1. Processing shall be lawful only if and to the extent that at least one of the following applies… e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.'

[7] JORF No 0160 of 13 July 2018 (the JORF being the official gazette of the French Republic).

[8] Article 59 of the LIL.

[9] Article 65 of the LIL. The SNDS was launched on 10 April 2017 and is a database merging together data from several health databases.

[10] Genetic data is defined as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question' (Article 4.13).