'Big data analytics' and processing of health data for scientific research purposes : Luxembourg’s legal framework

Research Protocol by Mahault Piéchaud Boura, time.lex

in Brussels, Belgium, March 2018 and updated in August 2018

Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

1. Overview of the legal framework

First, we would like to get an overview of the current and upcoming legal framework applying to the processing of health data for research purposes in your country.

a. The legislative and regulatory instruments regulating the processing of health data for research purposes (current regime)

What are the relevant applicable provisions governing the processing of health data in your country? Please provide online references (also to an English version, if available), a brief description and any specific relevant information.

Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data

This is Act regulated the processing of personal data in Luxembourg. It replaced the original text adopted in 1979. The 2002's Act transposed the 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 (the Directive). The implementation of the Act was supported by:

- Grand-Ducal Regulation of the 2 October 1992 on computer processing of medical data[1] « réglementant l'utilisation des données nominatives médicales dans les traitements informatiques »
- Commission Nationale de Protection des Données's Rules of functionning : Règlement intérieur adopté par la « Commission nationale pour la protection des données », ci-après dénommée « Commission nationale », par délibération n° 001/2002 en date du 29 novembre 2002, en application de l'article 35 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommée «la loi du 2 août 2002 ».

Act of the 28 August 1998 on Hospital Establishments[2] (loi sur les établissements hospitaliers) contains provisions on research made in health establishment and in particular opinion of the Ethic committee for research, which must be asked for any medical research project, this act also contains provisions on rights of patient to protection of their privacy in Article 38.

Act of 24 July 2014 on the Rights and Obligations of the patient[3],this Act contains provision on the information of the patient but also on the medical file and data of the patient (Article 15 to 19)

[1] http://data.legilux.public.lu/eli/etat/leg/rgd/1992/10/02/n2/jo

[2] http://data.legilux.public.lu/eli/etat/leg/tc/2011/05/24/n1/jo

[3] http://legilux.public.lu/eli/etat/leg/loi/2014/07/24/n2/jo

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Act of the 3 December 2014 on public research centres (loi ayant pour objet l'organisation des centres de recherche publics). This act governs public research institution in Luxembourg. It is relevant to this study in particular because it creates an Institute "Integrated Biobanks of Luxembourg".

Health Code: the Health Code is a compendium of the existing legislation in the field of health, but it is not the product of a codification exercise. It brings together all Acts and Regulation relevant to health, some of which also apply to scientific research and data processing.

Criminal code: the Criminal Code contain specific provision regarding frauds in the field of information technologies.

- Articles 509-1 to 509-7 « de certaines infractions en matière informatique » ;
- Article 458 on professional secrecy.

Social Security Code[4]: this code contains provisions applying to the share medical files.

- In particular Article 60 quarter on the « dossier de soin partagé ».
  - The Regulation for the implementation of this provision is being drafted.

There is also a compendium of all relevant text to digital identification: http://data.legilux.public.lu/file/eli-etat-leg-recueil-identification_numerique-20170715-fr-pdf.pdf

Shared electronic health records are indirectly relevant in this context because they can potentially be an important source for health-related research. Do shared electronic patient records exist in your country? How is the sharing of electronic patient records regulated? Can data stored in these records be used for research purposes?

The digital medical file of the patient finds its legal basis in Article 15 of Act of the 24 July 2014 on rights and obligations of the patients and in Article 60quater Social Security Code.

This electronic medical file aims to facilitate the treatment of one patient by several health professional and to avoid redundancies on the treatment prescribed. The access to the file is limited to the patient, the general practitioner of reference and the other doctors and health professional involved in the treatment of the patient.

A grand-ducal regulation is being drafted on the use and management of the shared medical file.

b. Revision of the current legal framework under the GDPR

How are the necessary changes to the national data protection framework, introduced by the GDPR, addressed in your country? What is the adopted legislative approach?

[4] http://data.legilux.public.lu/file/eli-etat-leg-code-securite_sociale-20170101-fr-pdf.pdf

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Is the GDPR implemented in your country by an entirely new legislative text or via amendments to the current data protection law? Please explain.

In preparation for the implementation of the GDPR a new Personal Data Protection Bill has been presented to the Chambre des Députés in December 2017 and adopted the 26 July 2018[5]. The new Act Protection Act[6] (hereafter NDPA) deals mainly with the new statute of the CNDP and some specific provisions, as allowed by the GDPR, pertaining to data processing and freedom of expression, processing and scientific research and processing of special categories of data by health services' professional.

What are the main characteristics of the legislative implementation of the GDPR in your country?

The NDPA abrogates the former Act on Data protection. Various institutions were consulted for the legislative process. The CNDP and the Conseil d'Etat expressed some reservations on the section about processing of sensitive data by health services' professional of the initial draft bill. Those reservation were lifted after extensive modification of the text.

What is your own assessment of the legislative approach adopted in your country for implementing the GDPR?

Legislative file can be found here: http://www.chd.lu/wps/portal/public/Accueil/TravailALaChambre/Recherche/RoleDesAffaires?action=doDocpaDetails&backto=/wps/portal/public/Accueil/Actualite&id=7184

c. The national data processing authority

Can you provide a short description of the role of the data protection supervisory authority in your country in the domain of processing health data for research purposes under the current legal framework?

The Commission Nationale pour la Protection des Données is a public establishment under the responsibility/ supervision of the Minister.

The law requires the CNPD to carry out a number of duties:

- to supervise and check the legality of collecting and using the data to be processed and to inform the parties carrying out the processing of the obligations incumbent on them;

[5] The Bill has yet to be formally enacted, however for clarity purposes this report will refer the New Data Protection Act nonetheless. The legislative file can be found here: https://www.chd.lu/wps/portal/public/Accueil/TravailALaChambre/Recherche/RoleDesAffaires?action=doDocpaDetails&id=7184&backto=p0/IZ7_28HHANET20F2A0A91N6L0M0CE3=CZ6_D2DVRI420G7Q402JEJ7USN3851=M/#Z7_28HHANET20F2A0A91N6L0M0CE3/%3E

[6] This was enacted on the 1 August 2018, http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- to ensure the observance of personal freedoms and fundamental rights, particularly as regards to privacy, and to inform the public of the personal rights involved;
- to receive and examine complaints and requests for checks on the legality of processing;
- to advise the Government on the subject[7].

Can you describe the adopted or proposed changes to this role of the national data protection authority to ensure compliance with the GDPR?

The task and power of the CNDP are those listed in Article 57 and 58 of the GDPR. It includes investigative and corrective powers, but also authorisation powers. The new attributions of the CNPD are wider that those under the current framework.

2. Transposition of Article 8.4 of Directive 95/46

Article 8 of Directive 95/46 prohibits, in principle, the processing of special categories of personal data concerning health. Article 8.2 lists a series of exceptions to this general prohibition. Article 8.4 states "*Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority*".

When transposing Directive 95/46 did your national legislator or supervisory authority make use of the power granted to Member States in Article 8.4 of the Directive? Did the legislator use this provision to insert any additional (i.e. additional to the exceptions listed in the Directive) exemption (to the prohibition to process health data) for the processing of health data for research purposes?

If yes, how is such an exemption formulated? Please explain.

The act distinguished between the processing of special categories of data and the processing of special categories of data by health services. In the second categories of processing, the operations may only have concerned data concerning health and sex life.

a. Transposition of Article 8.4 of the Directive 95/46

What are the exceptions to the prohibition of processing sensitive data? Do any of these exceptions address scientific research in the field of health?

- **How is such an exception formulated, and does it set out specific conditions?**

[7] Article 32 to 37 of the 2002's Act

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Act included genetic data in the definition of special categories of data. According to Article 6(1) genetic data could be processed only in the circumstances listed in Article 6 (3).

Article 8 of the Directive was transposed in Articles 6 and 7 of the 2002's Act. Article 8(4) provided the opportunity for additional exemption to the prohibition of sensitive data' processing. The 2002's Act provided a few additional grounds for the processing a special categories of data. In particular in Article 6(2)(g) "*the processing is necessary in the public interest for historical, statistical or scientific reasons without prejudice to the application of Article 7 hereafter*". This exemption was also applying to genetic data, if the processing was necessary for public interest motives such as scientific research.

Moreover Article 7 of the Act governed processing of data concerning health and sex life by health services. This constituted and additional exemption. Article 7 set particular condition to processing of sensitive data by "health services"(which are not defined) processing for medical and therapeutic purpose (1), processing for the management of health care service (3) but more importantly "*(T)he processing of data on health and sex life necessary for the purpose of healthcare or scientific research may be carried out by the medical authorities, or by the research bodies or the natural or legal persons whose research project has been approved under the legislation applying to biomedical research. If the controller is a legal entity, it shall indicate a delegated controller, who shall be subject to professional secrecy;*"

We notice that health professional could only processes two categories of data for research purposes and this could only be done in the frame of research projects approved under the legislation applying to biomedical research.

Moreover, in application of the Grand-ducal Regulation of the 2 October 1992 on the use of medical nominative data in digitalised processing, processing of medical data for medical and scientific research purpose could only be done through depersonalised (dépersonnalisées) data (article 13). If, however, the use of nominative data was absolutely necessary for medical and scientific research specific and legitimate needs, the collect and processing could only be done with the written consent of the data subject, whom would have been informed of the purpose of the processing. Further processing for a different purpose was not possible.

b. The regime applying to the processing of personal data for health research purposes

Is there a specific regime applying to data processing for research in the field of health purposes? What is the scope? Which are the steps, and who are the key actors?

Processing of personal data had to be notified to the CNDP by the data controller (Article 12 (1) (a)). But, there was an exhaustive list of processing activities exempted of the obligation of notification (art 12 (3)), this list included processing for therapeutic purpose and processing carried out by hospital establishment for the creation and update of medical files. Additionally, processing operations carried out by a single controller for same purposes could be dealt with in a single declaration (Article 12 (1)(b)). The modalities of the notification were defined in Article 13:

The notification was submitted prior to the processing, it contained the name and address of the data controller, the legal ground of the processing, its purpose, a description of categories of data subjects, and the data or categories of data linked. The notification also contained the recipient or categories of recipients to whom the data could be transferred, as well as the third countries to which the data would be transferred. And finally, the notification included a general description of the safety measures to be taken in application of the security

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

requirements set by Articles 22 and 23 of the Act, so that the CNDP could appreciate whether they were appropriate or not.

The declaration was done on paper, with a computerised document or an electronic transmission if necessary. The receipt to the declaration would be acknowledged by the CNDP. However, this declaration was subjected to a fee, set in a Grand-Ducal Regulation[8] of EUR 125. That fee could be reduced to EUR 100 if the declaration was also done in digital format. The commission registered and validated the notification. The three members of the CNDP had to be present for the deliberation to be valid[9]. The processing could start afterwards, once the controlled received a receipt form the CNPD.

However, for some categories of processing, an authorisation was necessary in application of the article 14 of the Act. This is applicable in particular to:

- Processing of genetic data for research purpose;
- Further processing for research purpose (when the purposes of the two processing were incompatible);
- Combination of two or more data sets;
- And "*the usage of data for purposes other than those for which they were collected. Such processing may be carried out only where prior consent is given by the data subject or if it is necessary to protect the vital interest of the data subject.*"

The application for the prior authorisation must have complied with the conditions set in Article 14 (3). The requirements were the same than for the declaration. The CNDP registers, validate the application for an authorisation and deliberates. The three members of the CNDP had to be present for the deliberation to be valid (see above).

As for the notification, there was a possibility for a single authorisation is foreseen in Article 14 (5). Processing having the same purpose, concerning the same data or categories of data, having the same recipient or categories of recipient could be authorised by the CNPD by a single authorisation.

From which generally applicable data protection provisions are researchers exempted and under what conditions? For what reasons? From which provisions? What are the consequences?

The 2002's Act foresaw situations in which the rights of information of the data subject could be limited. This applied also to scientific research if "*it [was] not possible to notify the data subject or doing so entails disproportionate efforts, or if the recording or the notification of the data is provided by law*".

Moreover, if there were obviously no risk of breaching the privacy of the data subject, the right of access could be limited by the controller "*when the data are being processed solely for the purposes of scientific research, or are stored in data form for a period not exceeding that necessary for the sole purpose of establishing statistics, and the*

[8] Grand-Ducal Regulation of 21 December 2007 (fees for prior authorisations).

[9] Rules of functioning of the CNDP, Règlement intérieur, Article 7 and 13.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

said data cannot be used for the purpose of taking a measure or a decision relating to specific persons". But in this case the controller would have to explain the reasons for which the right of access was delayed or limited.

c. Are there additional specific conditions governing the processing of data for scientific research purposes?

What are the suitable safeguards applying to the exemption foreseen by Article 8.4 of the Directive in your country?

Are there any specific provisions concerning: (i) professional secrecy, (ii) express consent for specific data, or specific provisions for (iii) deceased data subjects, or (iv) specific provisions for minors or persons subject to guardianship?

Are there specific requirements about the data subject's information? Or the person from whom the data was collected?

Are there specific penalties if the conditions for processing for scientific research in the field of health purposes are not respected? What do those penalties entail?

The Directive required suitable safeguards for any additional exemption to the prohibition set in Article 8. In the case of processing of special categories of data for scientific and medical research, Article 7 of the Act set out the requirements.

In principle processing of medical data for research purposes could only be done with "depersonalised" data. This meant anonymised or pseudonymised data. But there were exceptions to this principle, as seen above. Furthermore, genetic data and nominative medical data could only be processed for scientific purpose with the written consent of the data subject. Additionally, according to Article 7 (2) the data controller, or its delegate, had to be subjected to professional secrecy. Indeed, Article 7 applied to health services, whose staff are bound by professional secrecy. It follows that the controller or its delegate had also to be bound by professional secrecy.

Moreover, depending on the risks for the privacy of the data subject, but also depending the technical possibilities (state of the art) and the cost of their implementation, the data controller had to foresee technical and operational measures to ensure the protection of the data. More specifically, the measures should have prevented unauthorised access to facilities, unauthorised copy and/ or modification or unauthorised use. These measures should also have guaranteed that access be limited according to competence, that a log of the access to the data be maintained, and that data be safeguarded in a backup[10].

The research project had to be in conformity with legislation applicable to biomedical research. In application of Article 25 of the Act governing hospital establishments, research involving the human person had to be sanctioned

[10] Article 23 of the Act

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

by the CNER[11], the National Research's Ethic Commission. The Committee had sixty days to deliver its opinion. It is only after the deliverance of a favourable opinion that the research project could proceed.

Finally, breach of the provisions of Articles 6 and 7, or breach of confidentiality and security rules were sanctioned by an imprisonment from 8 days to a year and a fine from EUR 251 to EUR 125.000.

3. Further processing of health data (for research purposes): the current regime

a. How is the notion of further processing regulated in your national framework?

Article 4 of the Act allowed further processing. However, the further processing's purpose had to not be incompatible with that of the initial processing. Just as the "initial" processing, further processing was governed by the principles of purpose limitation, data minimisation, accuracy and storage limitation. Moreover, the Act stated that "*further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible with the purposes specified for which the data was collected*". This means that processing for scientific purposes was *de facto* considered compatible with the "initial" processing.

Are there specific conditions for further processing for scientific research in the field of health purposes?

Further processing for scientific purpose, as provided by the article 4(2) of the Act required the authorisation of the CNDP[12]. The authorisation procedure was the same as for an "initial" processing.

What are the rights of the data subject when it comes to such further processing?

The data subjects must have been informed in conformity with Article 26(2) of the Act. This meant that data subjects must have been informed at the latest when the data was transferred for further processing of the identity of the controller or its representative and the purpose of the further processing. Additional information could also be given to the data subject such as the categories of data concerned, the recipient of the data, the existence of a right of access and the possibility to rectify the data concerning him or her. However, such additional information of the data subject may not have been necessary. Indeed, the necessity of additional information was assessed with regard to the circumstances of the processing in order to guarantee fair processing vis à vis data subjects.

[11] http://legilux.public.lu/eli/etat/leg/loi/1998/08/28/n1/jo

[12] Article 14 (1)(c) of the Act.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Moreover, data subjects had a right of access to the data concerning them in application of the Article 28 of the Act. However, data subjects had to state a legitimate interest. This right of access included the right to any available information on the origin of the data.

What about the data subject's rights and further processing for scientific research purposes?

Not relevant because the regime applied was the general regime.

4. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes

Under the GDPR the processing of health data for research purposes is regulated by Article 9(2)(j), which authorises the processing of health data if this "*processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)* ***based on Union or Member State law*** *which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*" (emphasis added), and is combined with Article 89(1) ("*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner")*.

a. The impact of the GDPR on the rules applying to processing for research in the field of health

Please provide a summary of the main relevant characteristics of the new law/Bill (as far as it is relevant for processing health data for research purposes). How is (or will be) Article 9(2)(j) implemented in your country?

The data processing for scientific research purposes is organised in Articles 63 to 66 of the new Data Protection Act (NDPA). The processing of special categories of data, such as health data, is allowed for scientific research purposes only if the conditions set in these Articles are met. Furthermore, derogations to certain data subject rights are possible, if their exercise would render impossible or seriously impair the processing's purposes, and if appropriate guarantees are implemented.

In principle, the guarantees implemented by controllers should be proportionate to the nature, scope and purposes of the processing as well as the probability and level or risks for data subjects.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

b. Modification to the processing authorisation procedure applying to research in the field of health

How will the processing authorisation procedure (if any exists) be affected by the implementation of the GDPR? Can you describe any such change?

- **Is it a logical change?**
- **Is the supervisory authority involved? If yes, how?**

The GDPR introduces a change of logic, and prior notification and prior authorisation are marginalised. Henceforth, data controller will have to demonstrate the measures taken to ensures the compliance with the law and ensure the privacy of the data subject *a posteriori*, in the event of a control by the supervisory authority. The Bill set additional requirements for the controller of a processing activity with a scientific purpose.

Depending on the nature, scope, context and purpose of the processing, as well as the risks for the rights of the data subjects the data controller of a processing for scientific purpose must implement additional measures laid down in Article 65 NDPA. This apply to health professional and researchers alike. The additional measures are the following:

- Designation of a Data Protection Officer;
- The realisation of a Data Protection Impact Assessment;
- Anonymise or pseudonymise, and generally ensure the data cannot be used to take decision and action about and against the data subject;
- State of the art cryptography;
- Use of technologies reinforcing the protection of privacy;
- Restrict the access to the data;
- Established records of the data consulted, used, modified or deleted;
- Training of the involved staff on privacy, data protection and professional secrecy;
- Regular evolution of organisational and technical measures in place through external audits;
- Preparation in advance of a data management plan;
- Adoption of code of sectorial conducts (as laid down in the GDPR).

Controller must document and justify the decision to exclude one or more of the security measures listed in Article 65. It is the responsibility of the controller to asses which measure are necessary.

The new regime changes the logic that was applied so far. The CNDP no longer intervenes before the processing. The declaration, and authorisation prior to the processing will be the exception. The principle will be that the controller after having assessed the risks and taken the appropriate measures will proceed with the processing,

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

unless substantial risks remain, in such instance the CNDP will have to be consulted. The logic of the new approach brought on by the GDPR is that of a posterior control performed by the CNDP.

What about the right of the data subject and the obligations of the controller?

The rights of the data subject are those set in the GDPR. The NDPA admits the limitations envisaged in the article 89 (2) of the GDPR to the rights of access, right of rectification, rights of restriction of processing and the right to object. However, such limitations are conditioned by the implementation of technical and organisational measures to ensures the safeguards of the fundamental rights of the data subject. Moreover, these limitations can be implemented only if the rights in question would render impossible or seriously impair the achievement of the scientific purpose. However, the limitation must be proportional to the purpose of the processing, as well as the nature of the data processed and the nature of the purpose. We must observe this is left to the appreciation of the controller, and that the CNDP may exercise its powers of control *a posteriori*.

The obligations of the controller are set in the GDPR, the data subject must be duly informed, and the processing can only take place if appropriate technical and organisational measures to ensure the security of the data and safeguard the rights and freedoms of the data subjects are in place.

5. Further processing for research purposes under the GDPR

Further processing of personal data for scientific research purposes is regulated in the GDPR by Article 5(1)(b) ("*further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*") and Article 89(1) ("*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*").

Given the regime applied to further processing in the GDPR, can you describe the consequences, if any, in your national legal framework?

The new legal framework does not provide any specific provisions for further processing.

a. Health data sources for research purposes

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

This section seeks to identify information on the availability of health data for research purposes. Do public authorities or other entities facilitate the availability of health data for research purposes? In what way? Under what conditions?

b. Sources of data and their regulation

What are the different sources of health data that can be used for research purposes?

According to the Grand-Ducal regulation of 2 October 1992 concerning the use of nominative medical data in digital processing, Article 13, the processing was be done with depersonalised data, which meant anonymised data. However, if nominative or identifying data were necessary, the data subjects must have given a written and informed consent (Article 14).

- **DIRECT COLLECTION FROM THE PATIENTS:**

Under the current legal framework: please explain the currently applying rules that a researcher, who intends to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.), should follow.

Collect and processing of health data obtained directly from the data subject, i.e. the patient falls under the scope of Article 7 of the Act.

If the processing's purpose was solely medical and therapeutic then neither a notification or an authorisation was necessary. However, if the purpose was scientific research a declaration to the CNDP, in conformity with Articles 12 and 13 was necessary. Moreover, the project research must have complied with the applying legislation on biomedical research and have been validated by the CNER.

However, if the data collected for the research project included genetic data, then the authorisation to process had to be asked to the CNDP prior the beginning of the processing authority.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Under the GDPR, the data controller must perform a Data Protection Impact Assessment and implement additional measures as listed in Article 65 NDPA. Moreover, scientific research must be approved by the CNER, in conformity with the Hospital Establishment Act.

- **COLLECTION FROM HEALTH PROFESSIONALS AND HEALTH INSTITUTIONS:**

Under the current legal framework: please explain the rules currently applying that a researcher, who intends to obtain health data from medical staff, hospitals, etc., should follow.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The collect of data concerning health from health professionals and health institution and there processing required the authorisation of the CNDP. Moreover, the communication of nominative medical data can only be done with the written consent of the data subject.

Additionally, the research project necessitating the processing operation had to obtain the approval of the CNER in conformity with the Hospital Establishments Act.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Under the GDPR, the data controller must perform a Data Protection Impact Assessment and implement additional measures as listed in Article 65 NDPA. The scientific research purpose is presumed compatible with the initial processing purpose, which in the case of health professionals and health establishment is most likely medical and therapeutic purpose.

Moreover, scientific research must be approved by the CNER, in conformity with the Hospital Establishment Act.

- **PRIVATE DATABASES**

Under the current legal framework: please explain the rules currently applying for the setting up of and the use of a private database with health data for research purposes.

The constitution of private data base was based on the informed consent of the data subject. The data controller had to implement particular proportional safety measures, and declare the data base to the CNDP, in application of Articles 12 and 13.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Under the GDPR, the constitution of a private database concerning health also requires the informed consent of the data subject. The data controller must perform a Data Protection Impact Assessment and implement additional measures as listed in Article 65 NDPA. If the outcome of the Impact Assessment highlights risks for the privacy of data subjects, then the CNPD will have to be notified.

- **PUBLIC DATABASES**

Under the current legal framework: do public authorities make available health data for research purposes in your country and under what conditions?

IBBL – Integrated biobanks of Luxembourg was created by the Public Research Centre Act. For medical research purpose, the data processed must be depersonalised, that is at least pseudonymised. IBBL is linked to the Luxembourg Institute of Health (LIH) but the utilisation of the biobank's resources is independent of the LIH. This utilisation of the data is done in the respect of ethical rules as well as international security rules and must guarantee the confidentiality of the information of the data subject. Similarly, the National Cancer Register, governed by a Grand-Ducal Regulation and the Data Protection Act, is available for public interest research purpose.

If researchers are granted access to the resources of the IBBL or any other public database, they have to get approval of the CNER for their project to concretise. The CNDP will also have to be notified of the processing activities with

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

all the additional security measures implemented by the controller in order to guarantee the privacy of the data subject.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

IBBL grants or any other public data bases must grant to their resources. The research project must also be approved by the CNER in compliance of the legislation on biomedical research. The data controller must implement additional organisation and technical measures to ensure the privacy of data subjects and perform a Data Protection Impact Assessment. Depending on the outcome of the impact assessment the CNPD will have to be notified.

c. The application of the national framework to the AEGLE cases

This section seeks a short summary of the rules to be observed in your country by a hypothetical researcher involved in the AEGLE project. The objective is to obtain a practical response for informing such a researcher as clearly as possible.

1. Type 2 diabetes

The AEGLE project uses, after pseudonymisation, health data collected from patients who have expressed their consent with their data being used further for research purposes.

Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should the patient be informed about the new research project? Is a new patient consent, specifically focusing on the precise research project, required?

The AEGLE project would have had obtain the authorisation of the CNER for its research activities. The project must also have obtained the authorisation of the CNDP in application of Article 14 (1)(c) of the Act.

If the existing data bases -would have been combined, this should have been clearly mentioned in the application for the authorisation of the CNDP (Article 14 (1)(d) and Article 16 of the Act).

The project would also have had to demonstrate the implementation of appropriate state of the art safety measures, proportional to the risks paused to privacy and the costs of their implementation.

Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The project must obtain the authorisation of the CNER.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The GRPR regime must be implemented, DPIA must be performed and depending on the result the CNDP must be consulted. Moreover, the controller will have to implement additional security measures as listed in 65 NDPA. The controller will also have to document which measures where not implemented and for which reasons.

2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient's consent (after pseudonymisation).

Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other type of approval required? From which body? Should the patient be informed about the new research project?

According to Article 13, medical data processed for research purpose had to be depersonalised. Moreover, further processing for scientific purpose is not presumed incompatible to the purpose the data has initially processed. The AEGLE project could process the data collected for ICU purpose, however the project must be authorised by the CNER and the processing activity authorised the CNDP in application of Article 14 (1)(c) of the Act. Moreover, the data controller had implemented adequate technical and operational measures to ensure the privacy of the data subjects.

Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The AEGLE project must obtain the approval of the CNER for its research project, in application of Article 25 of the Hospital Establishment Act. Processing of scientific purpose benefits from an assumption of compatibility of purpose with the initial processing.

The GRPR regime must be implemented, DPIA must be performed and depending on the result the CNDP must be consulted. Moreover, the controller will have to implement additional security measures as listed in Article 65 NDPA. The controller will also have to document which measures where not implemented and for which reasons.

3. Chronic Lymphocytic Leukaemia (CLL)

The AEGLE project re-uses, after pseudonymisation, data coming from biobanks. In this instance, patients have given their informed consent for the samples and for the processing of their data. But this consent was given in general terms and not specifically for AEGLE.

Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should the patient be informed about the new research project?

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

AEGLE's purpose should not have been incompatible with the "initial purpose" for which the data were collected. However, according to Article 4 (2) of the Act further processing for scientific research purpose was not presumed incompatible with the specific purpose for which the data were collected. However, the data subject should have been informed at least of the identity of controller and of the purpose of the further processing (Article 26 (2)).

The project had to be authorised by the CNPD, because it was further processing for scientific purpose, but also because the AEGLE involved combination of various datasets (Article 14 (1)(d) and Article 16 of the Act). But before that, the research project had to be approved by the CNER.

Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

AEGLE research project will have to be approved by the CNER. The data controller must implement additional proportionate technical and organisational measures to ensures the privacy of the data processed. A DPIA must be performed and depending on the outcome the CNPD must be notified. The controller will also have to document which measures where not implemented and for which reasons.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU