# 'Big data analytics' and processing of health data for scientific research purposes : the Spanish legal framework

Research Protocol by Pedro Letai,
in Madrid, Spain *6 April 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

## a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018)

Under this heading we will provide an overview of the regulations applicable to personal data protection:

- **THE SPANISH CONSTITUTION**

In first place we must make reference to the Spanish Constitution[1]. Article 10 recognises the right to human dignity. In addition, Article 18.4 states that the law will limit the use of information technology to ensure the private and family life and reputation of the country's citizens, and the full exercise of their rights. These two precepts have given rise to the fundamental right to the protection of data of a personal nature, which has been defined as autonomous and independent by Constitutional Court Judgment 292/2000 of 30 November[2]. The Constitution reinforces the idea of the promotion of science and research by the public authorities[3].

- **ORGANIC LAW ON THE PROTECTION OF PERSONAL DATA[4].**

In development of the Constitution, Organic Law 15/1999 of 13 December on the Protection of Personal Data (the LOPD) was passed. The purpose of this law is to guarantee and protect the public freedoms and fundamental rights of individuals as regards personal data, and in particular their private and family life and reputation. The LOPD incorporates Directive 95/46 on Data Protection within the Spanish legal system[5].

The LOPD has been updated 4 times, twice in 2001, once in 2003, and subsequently in 2011.

The law defines data processing as all the operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and suppression, as well as the ceding of data resulting from communications, consultations, interconnections and transfers (article 3.c).

Likewise, decoupling procedure is defined as the processing of personal data in a way that the information obtained cannot be associated with an identified or identifiable person[6]. Decoupling means anonymisation procedure.

[1] 1978 Spanish Constitution. (Consolidated Text. Latest amendment: 27 September 2011).

[2] Constitutional Court Judgment 292/2000, of 30 November 2000. Unconstitutionality Appeal in relation to articles 21.1 and 24.1 and 2 of Organic Law 15/1999, of 13 December on Personal Data Protection.

[3] Article 44.2 of the Constitution.

[4] Organic Law 15/1999 of 13 December on the Protection of Personal Data .

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[6] Article 3.f of LOPD.



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 law is based on a series of principles that govern data processing. In first place, the LOPD defines the principle of the quality of the data, requiring them to be relevant to the purposes for which they were obtained[7]. Therefore, the gathering and processing of personal data must be based on its subordination to **proportionality in its processing**. The content of this law, which is of a fundamental nature, has been defined in Constitutional Court Judgment 292/2000. This judgment states that this fundamental right "seeks to ensure individuals have control over their personal data, their use and destination, with the aim of preventing trafficking of data that is illicit and damaging to the dignity and rights of the persons affected," establishing as regards its scope that "the purpose of protecting the fundamental right to the protection of personal data is not limited to the intimate details of a person but covers all types of personal data, whether private or not, when its knowledge or use by a third party could affect their rights, whether fundamental or not, because its purpose is not just to protect personal privacy, which is covered by Article 18.1 of the Spanish Constitution, but data of a personal nature."

This principle means that data of a personal nature can only be gathered for processing, and undergo such processing, if they are **adequate, relevant and not excessive** in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.

In addition, personal data subjected to processing may not be used for **purposes incompatible** with those for which they were collected. Therefore, the retention of personal data when they have ceased to be necessary or pertinent for the purposes for which they were gathered is contrary to the data quality principle.

Furthermore, personal data will be accurate and updated in such a way as to give a true picture of the current situation of the data subject. This means that if the personal data recorded prove to be inaccurate, either in whole or in part, they must be erased and replaced ex officio by the corresponding rectified or supplemented data, without prejudice to the rights granted to data subjects to rectify and suppress the data.

Lastly, the data quality principle prohibits the collection of data by fraudulent, unfair or illicit means.

Secondly, it is essential for the processing of personal data that the consent of the data subject be obtained[8]. This is defined as "any manifestation of free will that is unequivocal, specific and informed by means of which the data subject consents to the processing of their personal data." The law includes a series of exceptions to this unequivocal consent[9].

[7] Article 4 of the LOPD.

[8] Article 6 of the LOPD.

[9] Article 6.2 of the LOPD: "Consent will not be required where the personal data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities; where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment; where the purpose of processing the data is to protect a vital interest of the data subject, or where the data are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised".



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

Based on these characteristics, it can be determined that express consent is not required in every case. Nevertheless, in the case of the **data with special protection contemplated by Article 7 of the LOPD, such as data in relation to health, legislators have required that consent should be explicit in nature**[10]. º

The law requires that consent for the gathering should be freely given and informed, guaranteed by the prior information required by Article 5.1, that is to say, the data controller must declare in a clear and understandable manner the data that are to be processed and the purpose for which they will be used, so that the data subject can grant its consent freely and unequivocally.

The third obligation with regard to data processing is the right to be informed[11]. It is established that data subjects from whom personal data are requested must previously be informed explicitly, precisely and unequivocally of the following: the existence of a file or personal data processing operation; the obligatory or voluntary nature of the reply to the questions put to them; the consequences of obtaining the data; the possibility of exercising rights of access, rectification, erasure and objection; and the identity and address of the controller.

Nevertheless, an exception to the duty to inform is established **where explicitly provided for by law, when the processing is for historical, statistical or scientific purposes**, or when it is not possible to inform the data subject, or where this would involve a disproportionate effort in the view of the Spanish Data Protection Agency.

Another principle established in the LOPD is the principle of data security, which requires the processor to adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access[12].

Data processing also carries with it a duty of secrecy[13]. Any persons involved in any stage of processing personal data will be subject to professional secrecy as regards such data and this obligation will persist even after the end of the relations with the owner of the file.

Lastly, data controllers are under the obligation to enable citizens to exercise their rights of access, rectification, erasure and objection.

- **THE LOPD IMPLEMENTING REGULATION[14].**

The LOPD is complemented by RD 1720/2007 of 21 December, approving the implementing regulations for Organic Law 15/1999 of 13 December on the Protection of Personal Data (the LOPD Implementing Regulation).

[10]However, with the coming into force of EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), consent must be explicit in all cases.

[11] Article 5 of the LOPD.

[12] Article 9 of the LOPD regulated in Title VIII of the LOPD implementing regulation.

[13] Article 10 of the LOPD.

[14] Royal Decree 1720/2007, of 21 December, approving the implementing regulations for Organic Law 15/1999 of 13 December on the Protection of Personal Data.



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 regulation includes a series of provisions regarding data on health. These data are defined as information concerning the past, present and future physical or mental health of an individual. In particular, data concerning the health of persons is considered to include information on their degree of disability and their genetic information.[15]

As has been mentioned, the quality principle includes the shortest possible term for retention of personal data, which should be erased when no longer necessary or pertinent for the purposes for which they were to have been gathered or recorded. Nevertheless, data may be retained if they are first delinked, or exceptionally if according to specific legislation they are deemed to be of historical, statistical or scientific value.

Both the law and its implementing will be modified with the coming into force of the General Data Protection Regulation (GDPR).

- **DEVELOPMENT AND GENERAL COORDINATION OF SCIENTIFIC AND TECHNICAL RESEARCH ACT[16].**

For the purpose of establishing what should be understood by scientific uses, the LOPD refers to the National Plan for Scientific Research and Technological Development introduced by this regulation.

- **GENERAL PUBLIC HEALTH ACT[17].**

The aim of this law is to establish the basis for the population to attain and maintain the highest possible standard of health through policies, programmes, services and in general actions of all kinds by the public authorities, companies and citizen bodies with the purpose of acting on the processes and factors with the greatest influence on health. Personal information used in public health actions is to be governed by the terms of the LOPD[18].

- **BIOMEDICAL RESEARCH ACT[19]**

The aim of this law is to regulate biomedical research, fully respecting human dignity and identity and the inherent rights of persons. In particular, it regulates research using human beings that implies invasive procedures, research on human beings not implying invasive procedures, genetic analyses for clinical purposes, research using biological samples and biobanks, and research using embryos not related to assisted human reproduction.

The performance of any biomedical research activity will favour the health and welfare of the participant in the biomedical research and will respect fundamental rights and freedoms by means of guarantees of confidentiality in the processing of data of a personal nature and biological samples. As established in its Recitals, regulation of all these matters has taken into account the terms of the law on the autonomy of patients (*Ley 41/2002 Reguladora de la Autonomía del Paciente* - LAP) and the LOPD, which are recognised as additional sources in those matters not regulated by this Law.

The law establishes a series of guarantees for those participating in biomedical research. In the first place, the law requires the informed consent of persons who might participate, once they have received appropriate information,

[15] Article 5.1. g) of the implementing regulation of the LOPD.

[16] Law 13/1986 of 14 April on Development and General Coordination of Scientific and Technical Research.

[17] Law 33/2011 of 4 October, the General Public Health Act.

[18] Article 7 of the General Public Health Act.

[19] Law 14/2007 of 3 July on Biomedical Research.



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

which must be provided in writing[20]. The consent granted may be revoked at any time. Information must be received in advance in a clear manner, specifying matters such as the nature, extent and length of the procedures, preventive procedures available, measures for response to adverse situations, measures to ensure respect for private life and the confidentiality of personal data according to the requirements of data protection legislation, etc..

As well as ensuring compliance with personal data protection regulations, the law includes a series of specific provisions on the matter.

There are some important definitions in the LIB. For instance, article 3.c. states that anonymisation as the process whereby it is no longer possible to establish a link between data and the subject[21]. Thereby, anonymous data means registered data with no link with and identified or identifiable person. Accordingly, anonym data is defined as data that, as its origin or following processing, cannot be associated to an identified or identifiable data subject[22].

Nevertheless, LIB distinguishes between anonymised and pseudonymised data:

-Article 3.i defines anonymised data or irretrievably unlinked to an identifiable person as data that cannot be associated to an identified or identifiable person, through destruction of the link to any identifying information about the data subject, or because this association involves a disproportionate effort.

-Pseudonymised data or coded data is defined as data that are not linked to an identifiable person trough the replacement of or separation from all identifying information about that person by use of a code.

On the use of human biological samples for biomedical research purposes, the law is based on the consent of the source subject. On the matter of secondary uses of the biological samples of the source subject, as a general rule the use of data for purposes other than those for which consent has been granted is forbidden[23]. Nevertheless, samples may be used without the consent of the source subject when that consent cannot be obtained or when obtaining it would require an unreasonable effort. The duty of secrecy will persist even when the research or action has ceased[24].

Title V regulates other emerging matters related to the current growth trend in biomedical research, such as the performance of genetic analyses, access to and use of results and the obtaining and use of biological samples of human origin. In this regard, the Law lays down a series of guarantees in relation to the protection of data in genetic analyses and biological samples: guiding principles have been established on accessibility, equity and quality in the processing of the data, prior consent is required, and the situation of anonymised biological samples is contemplated.

Moreover, specific rules are envisaged in relation to deceased persons and pre-embryos and foetuses, for which data protection is also guaranteed, and duty of confidentiality is demanded.

[20] Article 4 of the Biomedical Research Act.

[21] Article 3.c of the Biomedical Research Act.

[22] Article 3.h of the Biomedical Research Act.

[23] Article 58 of the Biomedical Research Act.

[24] Article 5 of the Biomedical Research 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

- **BASIC LAW REGULATING PATIENT AUTONOMY AND RIGHTS AND OBLIGATIONS ON THE MATTER OF INFORMATION AND CLINICAL DOCUMENTATION[25].**

The basic law on patient autonomy (LAP) regulates the rights and obligations of patients, users and professionals, as well as the public and private health centres and services, on the matter of patients and clinical information and documentation.

The law establishes that all persons have the right to the confidentiality of the data concerning their health, so that nobody may access that data without prior authorisation according to the Law[26]. In addition, all actions within the scope of a patient's health need the free and voluntary consent of the affected subject[27]. Medical practitioners must inform patients of the relevant consequences of interventions, the risks and the contraindications, prior to the obtaining of consent.

Closely connected to the health data concept is the clinical records concept regulated in Chapter V of the LAP that defines it as "an instrument intended fundamentally to ensure adequate assistance for the patient," adding that "its principal aim will be to facilitate healthcare, placing on record all data that on the basis of medical criteria enable a truthful and current awareness of the state of the patient's health"[28].

The law regulates the right of access by patients themselves[29], by their family and by healthcare personnel[30]. In the case of the latter, the general rule is that healthcare professionals at the centre where the diagnosis or the treatment is being performed will have access to the clinical records as a fundamental element for the providing of adequate assistance, although certain limitations are imposed.

In addition, the LAP regulates the obligation for the clinical documentation to be retained in conditions that ensure its correct preservation and safety, although not necessarily on its original support, to provide adequate assistance to the patient for an appropriate period, at least 5 years as from discharge following each healthcare procedure[31]. In addition, healthcare professionals who perform their tasks on an individual basis are made responsible for the handling and custody of the healthcare documentation they may generate.

Special attention is paid to the consolidation of electronic formats in the handling of clinical records. The duality that exists between clinical histories in manual and electronic formats has led to the adoption of security measures in the implementing regulations of the LOPD. In the case of clinical records on paper, the centres responsible for such documents are required to implement a series of security measures that as well as being intended to prevent unauthorised access can help detect illicit information handling access. These security measures consist of the

[25] Law 41/2002 of 14 November -Basic law regulating patient autonomy and rights and obligations on the matter of information and clinical documentation .

[26] Article 7 of the LAP.

[27] Article 8 of the LAP.

[28] Article 15.2 of the LAP.

[29] Article 18 of the LAP.

[30] Article 16 of the LAP.

[31] Article 17 of the LAP.



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

establishing of a system for the recording of access to clinical documentation for which access is restricted exclusively to authorised personnel, with the establishing of methods that enable identification of accesses made in the case of documents that may be used by multiple users, and the registering of those cases where a priori unauthorised access has been gained to clinical histories, pursuant to a procedure that should be laid down in the Centre's Security Document.

This obligation to record accesses also exists for clinical histories handled in an automated or electronic manner. The Implementing Regulation for the LOPD requires that for each access attempt a record should be kept including at least the identification of the user, the date and time of the access, the file accessed, the type of access, and whether access has been authorised or denied. If the access has been authorised, it will be necessary to retain the information enabling identification of the record accessed. The identity of the person accessing the content of the clinical records will be revealed by the user name and password that the healthcare professions must use to read and/or modify clinical histories at the Centre[32].

Regardless of whether clinical histories are handled on paper or on IT systems, in addition to the above protocols or codes of conduct a Security Document must be drawn up by the healthcare centre. This Security Document is to consist of a manual detailing the technical and organisational measures adopted in accordance with current security requirements that must be complied with by personnel with access to the information systems[33].

- **GENERAL HEALTH ACT[34].**

The purpose of this law is to provide overall regulation for all the actions enabling effective implementation of the right to healthcare enshrined in Article 43 of the Constitution. It establishes that a fundamental activity of the health system is the carrying out of the epidemiological studies necessary to guide actions for the prevention of risks to health with greater efficacy, as well as healthcare planning and evaluation, and its basis should be an organised system of health information, vigilance and epidemiological action[35].

In each Regional Health Authority efforts should be made to achieve the greatest possible integration of information in relation to each patient, so that the principle of a single clinical health history for each individual must be adopted, at least within the limits of each healthcare institution. It should be at the disposal of the patient and the healthcare professionals directly involved in the diagnosis of the patient, as well as for the purposes of medical inspections or for scientific purposes, and the right of the patient to personal and family privacy must be fully guaranteed, as should the duty of secrecy binding all those with access to the clinical records[36]. In addition, the law establishes that hospital centres will carry out research and teaching duties according to the programmes of each Regional Health Authority, with the aim of complementing their activities[37].

[32] Article 93.1 LOPD Implementing Regulation: "the file or processing controller must adopt measures that ensure the correct identification and authentication of the users."

[33] Article 88 of the LOPD Implementing Regulations.

[34] Law 14/1986 of 25 April, the General Health Act.

[35] Article 8 of the General Health Act.

[36] Article 61 of the General Health Act.

[37] Article 68 of the General Health 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

- **ROYAL DECREE ON CLINICAL DRUG TRIALS[38].**

This provision applies to clinical trials with drugs for human use carried out in Spain. The law states that clinical trials must observe the patient data protection requirements of the LOPD[39]. In addition, it requires freely stated informed consent to be obtained from each of the trial subjects. It does however also contemplate a series of exceptions to the need for consent in certain cases[40].

- **SCIENCE, TECHNOLOGY AND INNOVATION ACT[41].**

This law is intended to promote research, experimental development and innovation as elements on which sustainable economic development and social welfare can be grounded.

Research staff providing their services in state universities, government research entities and the research institutions of other public administrations are required to adopt measures necessary for compliance with the applicable rules on data protection and confidentiality[42].

- **CRIMINAL CODE[43]**

The Criminal Code deals with a series of offences in relation to the right to data protection.

Firstly, the offence of seizure, use or amendment of recorded data carries a penalty of imprisonment of one to four years and a fine of twelve to twenty-four months for whoever without being authorised seizes, uses or amends to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telematics files or media, or in any other kind of file or public or private record. In the case of especially sensitive data, more serious penalties are established[44].

A special category of offence carrying a penalty of imprisonment of one to three years and a fine of twelve to twenty-four months is established for those who without having taken part in the discovery of the data, facts or images (and therefore without the need to participate in the conduct of the basic offence) although aware of their unlawful origin, were to disseminate, reveal or cede such data, facts or images to third parties[45].

[38] Royal Decree 223/2004 of 6 February regulating clinical drug trials.

[39] Article 3.2 of RD on clinical drug trials.

[40] Article 7.4 establishes such exceptions in cases of an immediate risk to the physical or mental integrity of subjects, when it is not possible to obtain their consent or that of their legal representative, or when the subjects are not capable of taking decisions because of their physical or mental state and they do not possess a legal representative.

[41] Law 14/2011 of 1 June on Science, Technology and Innovation.

[42] Article 15.1 l) of the Science and Technology Act and additional Provision Nine requiring mandatory compliance with the LOPD.

[43] Organic Law 10/1995 of 23 November on the Criminal Code.

[44] Article 197.2 of the Criminal Code.

[45] Article 197.3 of the Criminal Code.



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

There is an aggravated offence when the offences are committed by persons in charge of or responsible for the files[46].

There is also an aggravated offence based on the classification of the object or the victim. A penalty is established within the upper half of the sentence range when the disclosure or communication discloses personal data that reveals ideology, religion, beliefs, health, racial origin or sexual preference, or when the victim is a minor or lacks capacity[47].

Higher penalties are imposed if the acts are perpetrated for profit-making motives[48].

If the perpetrator is a public official, higher penalties are also envisaged, as well as permanent disqualification.

Lastly, Article 200 contemplates extending the privacy protection of the courts to the confidential data of legal persons.

## b. Revision of the current legal framework under the GDPR

On 10 November 2017 the Council of Ministers approved the Bill for the Organic Data Law for the purpose of adapting domestic legislation to the GDPR, thus replacing the current Organic Law.

Although it is true that the General Data Protection Regulation (GDPR) is directly applicable, its implementation within the Spanish legal system is required for the approval of other complementary domestic regulations so that its application can be fully effective.

The Bill is organised into nine titles containing seventy-eight articles, seventeen additional provisions, six transitional provisions, one derogatory provision and five final provisions.

Title I regulates the purpose of the organic law, which is to adapt the Spanish legal system to the GDPR. The principal development concerns deceased persons, as it allows heirs to access their personal data, as well as to rectify or erase them based on the instructions of the deceased.

Title II establishes that the data controller will not be responsible for incorrect information obtained on the data subject as long as all reasonable measures have been taken for them to be suppressed or rectified without delay, when the data has been obtained from another processor under the right to portability. It also expressly recognises the right to confidentiality, specific guarantees are regulated, and the principle of the minimisation of data is applied when it is considered that the processing of data by those lacking competence to do so is considered disproportionate. Within what is known as “lawfulness of processing,” specific reference is made to consent, which must derive from a declaration or a clear affirmative action by the data subject, excluding what had been known as “tacit consent.” If processing is for multiple purposes, it must be specifically and unequivocally stated that it is

[46] Article 197.4 of the Criminal Code.

[47] Article 197.5 of the Criminal Code.

[48] Article 197.6 of the Criminal Code.



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

granted for each one of them. The age from which minors can grant consent is set at thirteen, to place the Spanish system on the same level as that of other States in the region.

Regulation is also included on possible legal authority for processing based on compliance with a legal requirement made of the processor in the terms envisaged in the GDPR, when so established in a European Union rule or a law that might determine the general conditions for processing and the types of data covered by it.

Title III adapts to Spanish law the principle of transparency that regulates the right of data subjects to be informed regarding the processing. The organic law contemplates the rights to access, rectify, eliminate and object to personal data, the right to restrict processing and the right to data portability.

Title IV contains provisions applicable to specific processing. It incorporates certain situations in which the legislator presumes the overriding legitimate interest of the data controller in compliance with certain requirements, such as in the case of credit information systems. It also regulates situations in which there is evidence of public interest, such as those concerning video surveillance and systems for direct marketing opt-out ("Robinson lists"), public statistical purposes and internal denunciations in the private sector.

Title V refers to the data controller and the data processor. The model is one of active responsibility, which requires prior evaluation by the controller or the processor of the risk that might arise from the processing of the data, to then adopt such measures as may be appropriate. The figure of the data controller's representative acquires major importance in the GDPR and this is also reflected in the organic law, which is based on the principle that it may be mandatory or voluntary, included or not within the organisation of the controller or processor, and be a natural or a legal person.

Title VI in relation to international transfers of data adapts the provisions of the GDPR and refers to the procedures by which data protection authorities can approve contractual models or binding corporate rules, instances of the authorisation of a certain transfer and prior information requirements.

Title VII deals with the data protection authorities, which in accordance with the mandate of the GDPR must be established according to national legislation. Continuing with the scheme included in previous regulations, the organic law regulates the operation of the Spanish Data Protection Authority (AEPD) and considers the existence of the autonomous authority data protection entities and the need for cooperation among control authorities.

Title VIII regulates the "Procedures in the event of the possible infringement of data protection rules."

Lastly, Title IX regulates sanctions. It establishes a system of penalties that covers a broad range of infringements. It describes typical conducts and classifies them according to whether they are very serious, serious or minor, based on the classification in the GDPR.

The Bill plans for the repealing of the LOPD and those provisions of an equal or lower rank that contradict or oppose the terms of the GDPR[49].

[49] Sole repealing provision of the Bill.



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 text is based on the Opinion of the Council of State[50]. This Opinion made suggestions that it considered to be essential in relation to the content of several articles[51]. Matters analysed by the Council of State have included the presumption of accuracy of data obtained directly; the processing of data protected by law; verification of the identity of the data subject for it to exercise its rights; rights of access; processing related to the carrying out of certain commercial transactions; the Data Protection Officer (DPO); Codes of Conduct and appointment and the regulatory powers of the Directors of the AEPD. The text has also been based on the report on the analysis of the regulatory impact dated 10 November 2017[52].

## c. The national data processing authority

The Spanish Data Protection Agency (*Agencia Española de Protección de Datos* - AEPD) is the independent state control authority responsible for ensuring compliance with regulations on data protection. It ensures and oversees the fundamental right to the protection of personal data of the population.

The Agency is a Public Entity governed by private law with its own legal personality and full public and private legal capacity to act, exercising its duties with full independence from Public Administrations. It is connected to the Government through the Ministry of Justice.

Its regulation can be found in Title VI of the LOPD. The AEPD is governed by the LOPD and its own statute[53] .

Its functions are regulated in Article 37 of the LOPD. They include: to ensure compliance with the legislation on data protection; to issue the authorisations provided for in the Law; to issue instructions and recommendations; to consider applications and complaints; to provide information to persons; to impose penalties; to provide regular information on the draft general provisions set out in this Law; to obtain from the data controllers any assistance and information it deems necessary for the exercise of its functions, etc.

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

Chapter VI of the GDPR (Articles 51 to 59) regulates data protection control authorities. It lays down that each member State will establish that it will be the responsibility of one or several independent public authorities to supervise the implementation of the Regulation with the aim of protecting the rights and fundamental freedoms of individuals in relation to the processing and the facilitation of the free circulation of personal data in the European Union.

The regulation envisages the obligation of states to establish in law various aspects concerning the control authority.

In addition, it modifies the competencies and obligations of the control authorities of member states. These include: the duty to promote awareness in relation to data processing, controlling application of the regulation, advising of institutions and entities on legislative measures in relation to data protection; upon request, providing information

[50] Opinion of the Council of State of 30 October 2017. Number 757/2017.

[51] Specifically Articles 5, 9.3, 13, 14, 20, 21, 22, 26, 35, 39, 49, 53 and 56 of the LOPD.

[52] Report on the analysis of the regulatory impact of the draft bill for the organic law on personal data protection issued on 10 November 2017.

[53] Royal Decree 428/1993 of 26 March approving the Data Protection Agency Statute.



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 any interested party on the exercise of their rights, cooperating with other control authorities and providing of mutual assistance, encouraging the drawing up of codes of conduct, etc.

The Bill establishes the AEPD as an independent administrative authority connected to the government through the Ministry of Justice. The Bill modifies the provisions regarding the functions of the AEPD, which will perform the role envisaged in the GDPR[54]. The necessary cooperation and coordination with the corresponding autonomous authority data protection agencies is established[55]. Also, the AEPD will have to regulate specific matters that the Community Regulation has ceded to the national control authorities and will have to revise its personal data treatment to adapt it to those requirements.

# 2. Can you describe your national framework, as it results from the transposition of Article 8.4 of Directive 95/46:

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

Article 8 of Directive 94/46 refers to different types of data considered to be special[56]. Thus, data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life will not be processed. These data categories will be able to be processed when there is explicit consent from the data subject, when the treatment is necessary to protect the vital interests of the data subject or of another person, when processing is carried out during the course of the legitimate activities of a foundation, association or not-for-profit entity, as long as it exclusively concerns its members, and if processing relates to data manifestly made public by the data subject or were to be necessary for the recognition, exercise or defence of a right in court proceedings.

Nevertheless, Article 8.4 establishes that subject to the provision of suitable safeguards, Member States may, for reasons of significant public interest, lay down other exemptions either by means of domestic legislation or by a decision of the supervisory authority.

In Spain, the 1999 LOPD was responsible for transposing Directive 94/46. The processing of data with special protection related to health is regulated in Articles 7 and 8 of the LOPD.

Article 7 deals with data with special protection and sensitive data. In its first paragraph it makes reference to the mandate of the Constitution that nobody may be obliged to state their ideology, religion or beliefs, and if their consent is sought to do so, they should be warned of their right to refuse such consent.

[54] Article 47.1 of the Bill.

[55] Article 52 of the Bill.

[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.



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

On the matter of health-related data, Article 7.3 establishes that data in relation to health may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his explicit consent. It would appear that the only exception added to the Spanish legal system pursuant to the terms of Article 8.4 of the Directive is the processing of sensitive data when required by law.

Both in the data gathering phase and in the processing and ceding of data, the term "explicit" is understood to mean that a more explicit manifestation of the willingness to provide data is required, that is to say, express consent. However, unlike other categories of sensitive data, such as those related to ideology, beliefs or religion, it is not necessary for such consent to be stated in writing.

On the matter of data on health, doubts have arisen as to what specific data must be understood to be included under this heading. For example, data on alcoholism, drug dependency, relationship conflicts… From Directive 95/46 and Article 106 of European Convention 108 it can be determined that the concept includes information on past, present and future health, whether physical or mental, of an individual, and may concern information on a healthy, sick or deceased individual, and it should be understood that such data also include information on the examples indicated previously.

Article 7.5 envisages an exception to the need for explicit consent from the data subject. It establishes that these data can be processed in cases where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. Also, when processing is necessary to protect the vital interests of the data subject or another person if the data subject were to be physically or legally prevented from granting consent[57].

This system has two requirements: that the processing of the data should be necessary for prevention or medical diagnosis, the providing of healthcare or medical treatment or the obtaining of health services, as well as in situations in which it is necessary to protect the vital interests of another person when that person is lacks capacity, and that the data processing should be carried out by a health professional subject to the obligation of professional secrecy or by another person bound by an equivalent duty of secrecy.

Lastly, Article 8 establishes that health data may be processed by public and private healthcare institutions and centres and the corresponding professionals. Such institutions will be able to process such data in accordance with the provisions of the central or regional government on healthcare. In these cases, the rights of citizens in relation to the processing of their data gives way to the general interest represented by public health. The AEPD has declared that this article cannot be interpreted generically or extensively but must be restricted to cases where a regulatory provision specifically establishes or orders the processing of that data , or when it is indeed necessary and essential and it is justified in each specific instance (Report 0002-20001).

It should be mentioned that the General Health Act is considered to be the basic law applicable to the whole territory of the state except for those areas subject to regional government legislation. Its Article 23 states that when it comes to achieving objectives in the matter of public intervention in relation to individual or collective health, the health administrations may set up registers and perform such analysis and information-gathering as may be necessary to determine the various situations leading to intervention actions by the health authority. This article includes all the

[57] This exception derives from the exception in Article 8.3 of Directive 95/46.



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

operations included in the processing except for assignment. Therefore, the institutions, centres and professionals will be able to process the data of the patients attending them in accordance with the terms of health legislation.

It is also important to point out that although the processing of the health data of patients attending the centres does not require their consent pursuant to the terms of Article 8 of the LOPD, this does not absolve the data controller from the duty to inform the data subjects in the terms of Article 5.1 of the LOPD.

## 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?

Based on the above, there is no specific procedure in data protection rules on the processing of health data for research purposes. The regulations are those of the **LOPD,** which authorise the processing of data for research purposes when so provided for by law, when the data subject has given explicit consent, for the purpose of preventive medicine or diagnosis provided such data processing is effected by health professionals subject to professional secrecy, and in the case of healthcare institutions and health centres[58].

Note should also be taken of the implementing regulations of the LOPD, which as an exception to the application of the quality principle regulate a procedure authorising data to be kept even when no longer necessary or pertinent for the purposes for which collected. This procedure will always be initiated at the request of the controller wishing to obtain a declaration for the inclusion in a given treatment of data with historic, scientific or statistical values, as indicated in the LOPD and the RLOPD[59]. In the request addressed to the Director of the AEPD, the data controller should clearly identify the data processing for which the exception is being requested, expressly indicating the reasons for the declaration and outlining in detail the measures that the file controller proposes to implement to ensure the rights of citizens. The request should be accompanied by all the necessary documents and proof justifying the existence of the historic, scientific or statistical values justifying the declaration by the agency.

### Regulations on health data processing for research purposes are to be found in the rules applicable to the health sector.

In the first place, the Biomedical Research Act (*Ley de Investigación Biomédica* – LIB**)**. In its recitals it establishes the requirement to observe regulations on the matter of data protection in the regulation of biomedical research implying intervention on humans, as well as the carrying out of genetic analyses, the processing of genetic data of a personal nature and that relating to biological samples of human origin.

The LIB incorporates a series of rules on the protection of data. In first place, express written consent is required for the processing of genetic data for healthcare or research purposes. Therefore, the exception to the express consent of the subjects for the processing of their personal data in cases of preventive medicine or diagnosis or the

[58] Articles 7.3, 7.6 and 8 of the LOPD.

[59] Article 157 Implementing Regulations of the LOPD.



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

administering of healthcare services as long as they are performed by a healthcare professional bound by professional secrecy as envisaged in the LOPD will not apply. In the case of the processing of genetic data it will be necessary to obtain express consent in writing for personal data processing, which can be obtained using the informed consent form serving as a basis for the documenting of consent for the genetic analysis.

The law establishes the obligation to obtain the informed consent of those persons taking part in biomedical research, once the information that must be provided in writing has been received. This information must include matters such as: the nature, extent and length of the procedures, the available preventive procedures, measures to respond to adverse events, measures to ensure respect for the private life and confidentiality of personal data according to the demands of legislation on data protection, etc.

The law establishes a duty of confidentiality for the professionals and the obligation to retain genetic data. Personnel with access to genetic data are subject to the duty of secrecy on a permanent basis, and will only be able to transfer such data to third parties following express written consent, and this rule in turn links to the requirement that genetic data cannot be used for purposes other than those envisaged in the law itself or for commercial purposes. When the results cover several members of a family they must perform their communication individually, and guardians or representatives must do so in the case of minors. Lastly, the law conditions access by healthcare professionals at the centre or establishment where the patient's clinical records are held to their connection with the assistance provided to the latter and the pertinence of the knowledge of the information derived from the clinical records.

The system for obtaining, conserving, use and ceding of biological samples is also the subject of detailed regulation in the third chapter of this title. Logically, the legal framework again hinges on the consent of the subject that is the source of the sample and the prior information that must be provided to them[60].

Health professionals will be able to gain access to participant data in certain circumstances. First, they can access clinical histories to provide healthcare assistance. Second, for epidemiological, public health, research or teaching purposes, once anonymisation has taken place or express consent has been obtained from the data subject. Third, in exceptional circumstances in the general health interest, and once it holds a favourable report from the data protection authority, the competent authority will be able to authorise the use of coded genetic data, always making sure that they cannot be related to or associated with the source subject[61].

On the matter of the conservation of personal genetic data, the law establishes that they should be conserved for a period of 5 years. Beyond that time it will be able to be retained for research purposes in an anonymous manner, so that it is not possible to identify the source subject.

In short, the model established in the current code on the matter of biomedical research is based as a general rule on the express written consent of the data source, which may be waived in certain circumstances, either because it is not possible to identify the data subject because the data has been made anonymous as per Article 3i), following a favourable opinion from the Ethical Research Committee, or when it involves research linked to the initial research when it is considered that the purpose of such research is compatible with that for which consent had been granted. Except for those cases, according to the law express consent of the affected party would be required for any specific research.

[60] Article 58 of the LIB.

[61] Article 3.k of the LIB. (Coded genetic data or pseudonymised data)



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

Last, specific rules are envisaged in relation to deceased persons and pre-embryos, embryos and foetuses, regarding which data protection is also guaranteed and the duty of confidentiality is imposed.

The law on patient autonomy (*Ley de autonomía de paciente* – **LAP)** regulates the rights and obligations of patients, users and professionals, as well as those of public and private health centres and services on patient matters and clinical information and documentation.

The law establishes that everyone has the right to the confidentiality of data referring to their health, and that nobody may have access to them unless previously authorised according to the Law[62]. In addition, all actions within the sphere of a patient's health require the freely informed and voluntary consent of the affected party[63]. The medical practitioner must inform the patient of the relevant consequences of the intervention - the risks and the contraindications - before obtaining their consent.

The clinical record is defined as "the set of documents that contains the data, assessments and information of all kinds on the situation and clinical development of a patient over the course of the healthcare assistance."

Patients have the right to access clinical record documentation and to obtain a copy of the data held on it, limited only by the exceptions contained in section three of Article 18 of the LAP, which are: when harming the rights to confidentiality of third parties and the rights of the professionals participating in their preparation, who will be able to object to the right to access their subjective annotations. The LAP details a special procedure that should be established in each health centre to ensure this right is protected.

In the case of access by family members, consent from the data subject will be required, or the existence of a rule with the rank of law that permits it.

On the matter of access by medical staff, Article 16 of the LAP establishes as a general rule that healthcare professionals at the centre performing the diagnosis or the treatment of the patient will have access to the clinical record as a fundamental instrument for their adequate care, although it goes on to establish certain limitations:

- Access for legal, epidemiological, public health, research of teaching purposes is governed by the terms of the LOPD and the General Health Act and other applicable regulations. Access for these purposes requires keeping the patient's personal identification details separate from those involving clinical care, so that as a general rule anonymity can be assured, unless the patient were to have consented to not keeping them separate.

- Access to the data and documents of the clinical record is strictly limited to the specific requirements of each case. Personnel from the administration and management of the healthcare centres may only access the data of the clinical records related to their own duties. Duly accredited health staff performing inspection, evaluation, accreditation and planning tasks can have access to clinical records as part of their duty to verify the quality of assistance, the observance of patient rights or any other of the centre's obligations in relation to its patients or users or the administration of health services itself.

In addition, the LAP regulates the obligation to retain clinical documentation in conditions that guarantee its proper conservation and safety, although not necessarily on its original support, for due assistance to the patient during an

[62] Article 7 of the LAP.

[63] Article 8 of the LAP.



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

appropriate period of at least 5 years counted as from the date of initiation of each healthcare procedure[64]. In addition, healthcare professionals who perform their tasks on an individual basis are made responsible for the handling and custody of the healthcare documentation they may generate.

Special attention is paid to the consolidation of electronic formats in the handling of clinical records. The duality that exists between clinical histories in manual and electronic formats has led to the adoption of security measures in the implementing regulations of the LOPD. In the case of clinical records on paper, the centres responsible for such documents are required to implement a series of security measures that as well as being intended to prevent unauthorised access can help detect illicit information handling access. These security measures consist of the establishing of a system for the recording of access to clinical documentation for which access is restricted exclusively to authorised personnel, with the establishing of methods that enable identification of accesses made in the case of documents that may be used by multiple users, and the registering of those cases where a priori unauthorised access has been gained to clinical histories, pursuant to a procedure that should be laid down in the Centre's Security Document.

This obligation to record accesses also exists for clinical histories handled in an automated or electronic manner. The Implementing Regulation for the LOPD requires that for each access attempt a record should be kept including at least the identification of the user, the date and time of the access, the file accessed, the type of access, and whether access has been authorised or denied. If the access has been authorised, it will be necessary to retain the information enabling identification of the record accessed. The identity of the person accessing the content of the clinical records will be revealed by the user name and password that the healthcare professions must use to read and/or modify clinical histories at the Centre.[65]

Regardless of whether clinical histories are handled on paper or on IT systems, in addition to the above protocols or codes of conduct a Security Document must be drawn up by the healthcare centre. This Security Document is to consist of a manual detailing the technical and organisational measures adopted in accordance with current security requirements that must be complied with by personnel with access to the information systems[66].

**The Royal Decree on clinical drug trials** details the steps that must be taken for compliance by drug trials with data protection regulations. This rule regulates the consent that must be obtained from trial subjects. It is defined as a decision in writing that must be dated and signed for participation in a clinical trial voluntarily agreed by a person capable for giving consent after having been duly informed and documented on the nature, importance, implications and risks[67]. It also indicates how to proceed in the case consent cannot be granted and in the case of minors and those who are under age or lacks capacity.

It also contemplates a series of exceptions to the need for consent in the case of the specific interest in the clinical trial of the population where the research is being carried out and where it is justified for reasons of need for the

[64] Article 17 LAP.

[65] Article 93.1 LOPD Implementing Regulation: "the file or processing controller must adopt measures that ensure the correct identification and authentication of the users."

[66] Article 88 of the Implementing Regulation of the LOPD

[67] Articles 1 and 7 of the Royal Decree on clinical drug trials.



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

administration of the drug, such as cases of immediate risk to the physical or mental integrity of the data subject, or if the data subjects are not capable of taking decisions because of the state they are in[68].

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

### What are the suitable safeguards applied to the exemption foreseen by article 8.4 of the Directive in your country?

The LOPD contains a series of principles that must guide all data processing. Some of these principles contemplate exceptions in the case of data processing for research purposes. In first place there is the principle of data quality that requires the data gathered to be adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained. This means that the data being processed must not be used for purposes incompatible with those for which they have been obtained, and their retention when they cease to be pertinent is contrary to this principle. Nevertheless, an exception is contemplated when the processing is for historical, statistical or scientific purposes.

Secondly, it is essential for the processing of personal data that the consent of the data subject be obtained. Consent is defined as "any manifestation of free will that is unequivocal, specific and informed by means of which the data subject consents to the processing of their personal data". From these characteristics it can be determined that consent is not required in all cases. Nevertheless, in the case of the data with special protection contemplated by Article 7 of the LOPD, such as data in relation to health, legislators have required that consent should be explicit in nature. As a result, research studies that use personal data must obtain consent of the data subject on the matter of data protection, and this will complement the consent to submit to the research in question.

Thirdly there is a duty to inform the data subject. This duty is waived when expressly envisaged in a law, when the processing is for historical, statistical or scientific purposes, or when it is not possible to inform the data subject, or where this would involve a disproportionate effort in the view of the Spanish Data Protection Agency.

As a consequence of the principle of data security, research performed using health-related data must observe those rules classified as high level.

The storage, processing and handling of healthcare information must be carried out according to its purpose, using appropriate security measures to prevent unauthorised access or use. As specified in Royal Decree 994/1999 of 11 June approving the Regulation on security measures for automated filing systems containing personal data[69], these obligations include:

[68] Article 7.4 establishes such exceptions in cases of an immediate risk to the physical or mental integrity of subjects, when it is not possible to obtain their consent or that of their legal representative, or when the subjects are not capable of taking decisions because of their physical or mental state and they do not possess a legal representative.

[69] Royal Decree 994/1999 of 11 June approving the Regulation on security measures for automated filing systems containing personal data .



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

- Drafting of a security document for mandatory compliance by personnel with access to the data incorporated to the information system that specifies the protected documents, the measures intended to guarantee their security level, personnel duties and obligations and the procedures for handling incidents and making backup copies of the documents.
- Appointment of a person to be responsible for the security of the files making up the information system who will be responsible for controlling compliance with the security measures.
- Specification of the duties of each of the persons authorised to access the personal health data and the detailed information provided to them on the obligations arising from such access.
- Preparation and carrying of a register to record anomalies that affect or might affect the security of the data.
- Control of access and identification of the users accessing the system, verifying that they have the authority to use the information obtained from it for the performance of their duties, and the establishing of mechanisms to prevent access to resources other than those authorised.
- Following the taking of an inventory, storage of the support containing information of a personal nature in areas where access is restricted to personnel authorised to use it; preparation and control of backup copies of the information technology support containing such information, and the transfer of such support via data transmission systems when necessary, after encoding or the use of any other mechanism that ensures that such information is not intelligible by unauthorised third parties.
- Carrying out of regular IT audits to assess the adequacy of the security measures, identify the deficiencies of the system and recommend corrective measures.
- Custody and conservation of personal data must be entrusted to professionals bound by professional secrecy rules, to preserve the confidentiality of the personal data and thus the right to privacy of the persons to whom the data relates.

In addition the duty to secrecy is established.

Lastly, the data controllers are required to ensure the exercise of the rights of citizens to access, rectify, suppress or oppose their data.

These rights are entirely personal, independent and free of charge. Spanish Constitutional Court Judgment 292/2000 of 30 November establishes that "the fundamental right to which we refer guarantees individuals the power to control and dispose of their personal data. It grants data subjects a range of powers that are essential elements of the fundamental right to the protection of personal data, consisting of the rights of the data subjects to consent to the gathering and use of their personal data and to know them. To make such elements effective, data subjects have the right to know who holds their personal data and for what purpose, as well as the right to object to such holding and use, demanding that the person holding the data terminate the possession and use of such data."

The right to access implies requesting and obtaining, free of charge, information on data submitted for processing, their origin, as well as the communications made or intended to be made using them[70]. The right to access will be

[70] Article 15 LOPD.



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

exercised by means of a request addressed to the data controller, who will have a maximum term of one month to rule on the request for access.

In the case of clinical records, the terms of the right to access are regulated in Article 13.2 of the LAP, which states that: "The information will include the database information on the data subject and that resulting from any processing or computerised process, as well as the origin of the data, the transferees of the data and specification of the concrete uses and purposes for which the data are stored."

Cancellation and rectification rights, regulated in Article 16, recognise the right to suppress or correct personal data processed in a manner not in accordance with the terms of the Law, and in particular when they are inexact or incomplete. This rule must be considered in relation to the principle of data quality. Data must be exact and updated so that they truthfully reflect the current situation of the data subject. Therefore, if they were to be inexact, incomplete, unnecessary or not pertinent, they must be rectified, completed or cancelled, tasks that will correspond ex officio to the data controller, who will be required to be especially diligent in this regard.

## 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?

- **PROFESSIONAL SECRECY.**

Given the sensitive nature of health-related data, Article 7.6 of the LOPD establishes that the processing of the data is possible for prevention or medical diagnosis, the providing of healthcare or the obtaining of health services as long as it is carried out by a health professional subject to the obligation of professional secrecy or by another person bound by an equivalent duty of secrecy.

The specific laws regulating the processing of health data for research purposes also refer to professional secrecy. On the matter of access to clinical records by health professionals, the LAP establishes that when access to data is necessary to prevent risk or serious danger to the population, the health authorities may gain access to identified patient data. Access must be by a professional subject to the obligation of professional secrecy or by another person bound by an equivalent duty of secrecy[71].

For its part, the LIB establishes that personnel accessing genetic data in the exercise of their duties will be subject to the duty to secrecy on a permanent basis, and that only with the express written consent of the data subject will it be possible to disclose genetic data of a personal nature to third parties, a requirement linked to the principle of data quality, implying that is must not be processed for commercial purposes or purposes other than those envisaged in the law itself.

- **DECEASED DATA SUBJECTS**

The AEPD has ruled on whether the processing of deceased persons is covered by the LOPD. In its report of 23 May, 2003 it states that in the light of the terms of Spanish Constitutional Court Judgment STC 292/2000 of 30 November, "if the fundamental right to data protection is to be considered as the right of individuals to decide on the possibility of a third party knowing and processing data personal to them, which implies granting their consent to the

[71] Article 16.3 of the LAP.



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

processing, with the duty to inform and the exercise by data subjects of their right to access, rectify, suppress or object, it is evident that such a right disappears upon the death of the individuals, so that the processing of the data of deceased persons cannot be considered to be included within the scope of application of Organic Law 15/1999."

Various resolutions by the Agency have echoed this position. In a resolution dated 12 June 2007 in case E/344/2006, it stated that "the purpose of the LOPD is to guarantee and protect the public freedoms and fundamental rights of individuals in relation to the processing of their personal data, and in particular their private and family life and their reputation" as laid out in its Article 1. In addition, consideration should be given to Article 32 of the Civil Code, which states that the civil personality of individuals is extinguished upon their death. Deceased persons do not therefore possess the right to personal data protection according to the provisions of the LOPD.

In a similar manner the Implementing Regulation of the LOPD establishes that "this regulation will not apply to data concerning deceased persons." Nevertheless, this law contains a rule with an exception for the heirs of the deceased or other persons fulfilling the requirements established by the deceased to request the suppression of the data. The second clause of Article 2.4 of the Regulation states as follows: "Nevertheless, persons linked to the deceased, for family or similar reasons will be able to contact the data controllers or processors holding data on the deceased for the purpose of notifying the death, providing adequate proof of the fact, and where appropriate requesting the suppression of the data." Therefore, such requests by persons related to the deceased will not in practice constitute the exercise of the right to suppression regulated by Article 18 of Organic Law 15/1999, but rather will have as their purpose the notification of the error in the contents of the file, requiring the suppression of the data corresponding to the deceased.

Having analysed the provision of a general nature regarding deceased persons, analysis should now be made of the specific legislation in the case of research.

Article 18 of the LAP establishes that "healthcare centres and professionals acting on an individual basis will only grant access to the clinical records of deceased persons to persons with family or de facto links to the deceased, unless the deceased were to have expressly forbidden it and this fact is able to be demonstrated. In any event, access by a third party to clinical records motivated by a risk to their health must be restricted to the pertinent details. No information will be provided that affects the privacy of the deceased or of the subjective notes of the professionals, or that might harm third parties," The AEPD has specified that it will only be possible to access the clinical records of a deceased patient when the requesting party were to have been designated by the deceased to exercise the actions envisaged in LO 1/1982 on protection of the private and family life, reputation and the subject's image.

The LIB also contains provisions regarding the processing of data of deceased persons. Firstly, with regard to the donation of embryos or human foetuses, in the case of the death of the persons from whom the embryos came, it will be necessary for there not to be any express opposition[72]. Title V regulates genetic data of a personal nature. It establishes that in the health field, samples from deceased persons may be obtained and analysed as long as they are of interest for the protection of health, unless the deceased were to have expressly forbidden it when alive. Access by family members to information derived from the genetic analysis of the deceased will be limited to data pertinent to the protection of their health[73].

- **MINORS**

[72] Article 29.2 of the Biomedical Research Act.

[73] Article 48.1 of the Biomedical Research 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

In the case of the processing of data on minors, consideration must be given to the specific provisions in the Implementing Regulation of the LOPD on the matter. Therefore, as regards the granting of consent, point one of Article 13 establishes that "The processing of the data of children over the age of 14 will be allowed with their consent, except in those cases in which the law requires consent to be granted in the presence of those holding parental rights or legal guardianship. In the case of children under fourteen, the consent of parents or tutors will be necessary."

Therefore, consent for the processing of personal data will only be able to be granted by the interested party, unless the data subject is under the age of 14 or is lacks capacity, in which case it must be granted by the parents or guardian, notwithstanding the requirement for the consent to be backed by the latter even when the child is over 14, in those cases established by law.

The obligation to inform envisaged in Article 13.2 of the LOPD must be carried out with greater stringency when consent is to be obtained from a minor, as it is addressed to a person who has not reached adulthood, which justifies the need for its adaptation so that it is understandable to a child. In the words of Article 13.3 "When processing concerns data on minors, the information addressed to them must be stated in language that is clearly understandable to them, with express indication of the terms envisaged in this article."

Here mention should be made of the warnings contained in Article 13.2 of the Regulation in relation to the information that may be requested from a minor. The Article states that "in no case will data be obtained from the minor that enables the gathering of information on the remaining members of the family group, or on its characteristics, such as data in relation to the professional activity of the parents, financial information, sociological data or of any other kind without the consent of the owners of such data."

On the matter of evidence of consent, Article 12 of the Regulation states that "the data processor will be responsible for proving the existence of consent from the data subject by any means of proof admissible in law." In the case of minors, the Regulation is more demanding. Thus, Article 13.4 states: "it will be the duty of the data controller or processor to implement procedures that ensure that the age of the minor and the authenticity of the consent provided by the parents, guardians or legal representatives, as the case may be, have been duly verified."

Lastly, in relation to the exercise of so-called ARCO rights, the AEPD has ruled on whether the representation of a minor exercised by the holder of parental rights can be considered as duly evidenced representation for the purposes of the exercise of such rights. In Report 409/2004 in relation to the right to access the clinical records of minors by the holder of parental rights, when considering the case of minors aged over 14, Article 162 of the Spanish Civil Code states that they have sufficient capacity to exercise their ARCO rights personally, without the need for the intervention of their legal representatives. In the case of minors under the age of 14, Article 162 of the Civil Code will apply, taking into consideration their level of maturity.

Article 9.3 c) of the LAP establishes that consent is to be granted by the legal representatives when the under-age patient is not capable intellectually or emotionally of understanding the scope of the intervention. In this case, consent is to be given by the legal representative of the minor after having listened to his or her opinion if over the age of 12. In the case of minors who are neither disabled or lacks capacity, but are emancipated or are over the age of sixteen, consent is not to be provided by proxy. However, in the case of interventions implying serious risk in the opinion of the healthcare professional, the parents will be informed and their opinion will be taken into account when taking the corresponding decision".

In regulating informed consent, the LIB establishes that it is to be granted by proxy when the patient is lacks capacity or is under age. Nevertheless, patients will participate as far as possible in the taking of decisions during the course



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

of the research process[74]. In cases of the genetic analysis of several members of the family, the results will be notified individually, informing guardians and legal representatives in the case of minors[75].

When obtaining biological samples from minors for research purposes it must be ensured that the risk is minimal for the source subject, that significant knowledge regarding a sickness can be obtained from the research, that such knowledge cannot be obtained by other means, and the authorisation has been obtained from the legal representatives of the minor[76].

**The Royal Decree on clinical drug trials** also includes specific provisions with regard to minors. In the case of research with no potential benefit for the subject of the research when the subject is a minor, to avoid possible exploitation there will be no economic compensation paid by the developer of the research[77]. Clinical trials using minors will only be able to be carried out when they are of specific interest to the population being researched; the welfare of the subject will prevail over the interests of science and society; informed consent must be obtained; the protocol must be approved by a Clinical Research Ethics Committee formed by experts in paediatrics, and the directives of the European Agency for Evaluation of Medicinal Products are followed.

## Are there specific requirements about the data subject´s information or about the person from whom the data was collected?

Article 5 of the LOPD contemplates the duty of the data controller to inform the data subject at the time their personal data are gathered. This duty to inform must be satisfied even in those cases in which consent of the data subject is not required for the processing of their data.

The law makes a distinction between data collected from the data subject and that obtained from private entities, sources accessible to the public, and persons other than the data subject.

In the case of data provided by the data subject, the law considers there is implicit consent in the communication, although it first requires information to be provided detailing the rule so that the data subject is aware of the existence of the file, its consequences, rights and other matters referred to in the rule. The information provided must be of quality, that is to say, the data subjects must be informed expressly, precisely and unequivocally. The information must be given in such a manner that the data subject can be fully aware of the scope, content and consequences of the supply of the data and the rights that correspond to them. The information to be provided includes: the existence of the file, the purpose for which the data is gathered, the recipient of the information, whether the replies to the questions asked are voluntary or obligatory, the consequence of the obtaining of the data or the refusal to provide them, the possibility of exercising their ARCO rights and the identity and address of the data controller.

[74] Article 4.2 of the Biomedical Research Act.

[75] Article 51.2 of the Biomedical Research Act.

[76] Article 58 of the Biomedical Research Act.

[77] Article 3.8 of the RD on clinical drug trials.



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

In the case of data not obtained by the interested party, information must be provided within three months from the moment of registration.

As an exception, this information is not due when the treatment has historical, statistical or scientific purposes, nor when two requirements are fulfilled jointly: the data should have come from sources accessible to the public, and they should be destined for use for advertising or commercial research.

On the matter of specific rules on research in health fields, the LAP highlights in its recitals the importance of patient rights, which include the right to information, informed consent and the private nature of information in relation to a person's health. In addition, it stresses the importance of ensuring confidentiality of information in relation to healthcare services.

Although it is true that the duty to inform is of vital importance, there are other general interests such as epidemiological studies, situations of serious risk to the health of the community, research and clinical trials that when included in rules with the rank of law may justify a grounded exception to patient rights. Along these lines, the Council of Europe in its recommendation of 13 February 1997 on the protection of medical data, after stating that information must be gathered and processed with the consent of the affected party, indicates that information may be restricted if so established in a law and it constitutes a necessary measure in the general interest.

In Article 4, the LAP regulates the duty to inform for healthcare purposes. For the purpose of any action in the area of their health, patients have the right to know all the information available on the matter, except for those items excluded by the law. The owner of this right to healthcare information is the patient, although persons close to the patient may be informed as long as the latter allows it.

Article 6 of the LAP regulates the right of the population to be informed about health problems when they represent a threat to public health.

As a result, patients must be provided with the information indicated in Article 4 before the obtaining of consent for any action in the health sphere. This information must include the relevant consequences or significance, the risks relating to personal or professional circumstances, the probable risks in normal circumstances, and the contraindications. Patients can waive their right to be informed, as long as it is documented.

The **LIB** establishes the free will of individuals as the basis of the rights to provide consent and obtain prior information[78]. To this end, it guarantees the right to information and the protection of personal data and the duty of confidentiality. This being so, consent must be granted expressly in writing once the appropriate information has been received.

In the case of the obtaining of informed consent from persons participating in genetic analyses for research purposes, the law determines that notwithstanding the terms of the LOPD, the data subject must receive the following information in writing: purpose of the genetic analysis for which consent is to be given; place where the analysis will take place and the use of the sample; persons who will have access to the results of the analysis when they have not been subjected to a depersonalisation process; a warning on the possibility of unexpected discoveries, and a warning on the possible implications for family members.[79].

[78] Article 4 of the LIB.

[79] Article 46 of the LIB.



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

Once the research has been completed, if it gives rise to relevant information for the health of the participants it should be made available to them. The data controller must send a summary to the appropriate authority and to the research Ethics Committee[80]. In addition, the results of the research should be made public once concluded, always taking into account the provisions of data protection regulations.

## 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?

Article 44 of the LOPD details the infringements of its regulations and classifies them as minor, serious or very serious.

Minor infringements include: Failure on formal grounds to respond to a request from a data subject for the correction or suppression of processed personal data when legally due; failure to provide the Spanish Data Protection Agency with the information it requests in the exercise of the duties assigned to it by law in relation to data protection aspects of a non-substantive nature; failure to request registration of the personal data file on the General Data Protection Register, when this does not constitute a serious infringement; collection of personal data from the data subjects themselves without providing them with the information required by Article 5 of the law; failure to comply with the duty of secrecy established in Article 10 of this law, unless it constitutes a serious infringement.

Serious infringements include: creating of public files or the collection of data without officially published authority; creating of private files or gathering of data for improper purposes; collecting of data without the consent of the data subject; unlawful processing; obstruction of the rights of data subjects, breach of the duty of accuracy; breach of the duty of secrecy; infringement of security measures; breach of the duty to inform.

Lastly, serious infringements include: the collection of data in a misleading or fraudulent manner; ceding of data when prohibited, infringement of rules on data with special protection; failure to desist from unlawful use despite being asked to do so; breach of rules on international data transfers; unlawful treatment contrary to the exercise of fundamental rights; breach of the duty to secrecy.

Therefore, there are various categories of infringement in relation to the processing of health-related data. As mentioned in the first paragraph, one of the duties of the data controller is to establish the necessary security measures in relation to this data. Article 9 of the LOPD establishes the obligation of the controller or, where applicable, the processor to adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access. In the case of the data with special protection of Article 7 of the LOPD, section 3 of Article 9 refers to the rules governing the requirements and conditions to be met by the files and the persons involved in processing the data in those files. According to Article 44.3. h) it will be considered a serious offence if files, facilities, software or hardware containing personal data are held without the adequate security protection required by law.

In addition, data processing carries with it a duty of secrecy. The data controller and those participating at any stage of the data processing are bound by professional secrecy requirements regarding the data and the duty to keep such data safe. These obligations will persist even after the termination of their relationship with the owner of the file or

[80] Article 12 of the LIB.



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 data controller. Breach of the duty of secrecy constitutes a minor, serious or very serious infringement, depending on the nature of the data stored, as they require differing security measures.

On the matter of the processing of specially protected data, Article 44.4.c) considers the following to be very serious infringements: collecting and processing of the personal data referred to in section 2 of Article 7 without the express consent of the data subject; the collecting and processing of the data of Article 7.3 when not ordered by law or not expressly consented to by the data subject, and any breach of the prohibition contained in Article 7.4.

## d. Formalities prior to processing: the general regime under the current framework

The LOPD makes a distinction between publicly and privately-owned files. According to Article 5.1.l) of the RLOPD, private files are "those controlled by persons, companies or private law entities, irrespective of who owns their capital or the origin of their economic resources, as well as files controlled by public law corporations, as long as such files are not strictly associated with the exercise of public law powers attributed to them by their specific legislation."

Privately-owned files are regulated in Article 25 of the LOPD. This rule establishes that privately-owned files containing personal data necessary for the legitimate activity or purpose of the owning person, company or entity can be created as long as the guarantees established by the law for the protection of persons are respected. The principal requirement regarding the creation of files is that they should be registered, as established by Article 26 of the LOPD. This rule establishes that anyone creating a file with personal data should first give notice to the AEPD. Article 18 of Directive 95/46 establishes that Member States will provide that the controller or his representative, if any, must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. The minimum content for the notification is laid down: the data controller, the purpose of the file, its location, the type of personal data it will contain, security measures, the ceding of data and if applicable, transfers to third countries.

Article 5.1.m) of the RLOPD defines publicly-owned filing systems: files controlled by constitutional bodies with constitutional importance of the State or autonomous institutions with similar functions, local public administrations, as well as associated or dependent entities or bodies and public law Corporations, as long as their purpose is the exercise of public law powers." On the matter of the creation, modification or suppression of the files belonging to Public Administrations, these will require a general provision that must be published in the Official State Gazette or the corresponding Official Journal. These provisions regarding creation should include the following matters: the purpose of the file and the uses envisaged, the persons or groups from whom it is planned to obtain data of a personal nature, the procedure for the collecting of the data, the basic structure of the file and description of the types of data, the ceding of data, the Public Administration bodies responsible for the file, the services or units before which the rights to access, rectify suppress and oppose the data can be exercised, and the security measures. The law does not contemplate the registration of publicly-owned files, as they will be registered ex officio by the AEPD once the documentation for setting them up has been received.



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

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

The LOPD applies to personal data recorded on a physical support which makes them capable of processing, whether automated or not, and to all subsequent use of such data[81].

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

We must refer back to the principle of data quality in the processing of the data. Article 4 of the Law forbids the use of the data for purposes incompatible with those for which it was collected. In addition, the Implementing Resolution for the LOPD establishes that data of a personal nature may only be collected to comply with specific, explicit and legitimate purposes by the data controller. Such personal data may not be used for purposes incompatible with those for which they were collected.[82]. Constitutional Court ruling 292/2000 of 30 November establishes that incompatible should be interpreted restrictively, being assimilated to different from.

The general rule is that data should be erased once it is no longer to be used for the purpose for which it was collected. There is an exception in the case of data gathered for statistical, historical or scientific purposes. The procedure is developed in Chapter VII of Title IX of RD 1720/2007.

Nevertheless, the law establishes that subsequent treatment of the data for historical, statistical or scientific purposes is not considered incompatible, excluding it from the duty to inform of Article 5.5. According to the regulation, determination of those purposes will be based on the legislation applicable in each case.

The communication or assignment of data is regulated by Article 11 of the LOPD. For analysis of the legal clauses in relation to communication one must refer to the definition established in Article 3.i) of the LOPD. Thus, assignment or communication of data: any disclosure of data to a person other than the data subject.

The law establishes two requirements for the validity of the assignment or communication of data: the communication must reflect compliance with the purposes directly related to the legitimate functions of the assignor and assignee, and it should furthermore count on the prior consent of the data subject.

On the matter of the first requirement, the law requires that there be reasonable cause for the transfer based on the relevance of the transaction. As well as being directly related to the activity of the assignor and assignee, these functions must be legitimate. There are no exceptions to this requirement.

On the other hand, in the case of the second requirement, that for consent, the law establishes a series of cases when this will not be necessary:

-The first exception to the need for consent arises when the transfer is authorised under a law. For example, a law could authorise the entering into of certain contracts that because of their content imply the declaration of the data of third party to the other party to a contract.

-The second exception to the need for consent from the data subjects for disclosure of their data is when the data have been collected from publicly accessible sources. Article 6.2 on data subject consent establishes a similar exception in that such consent is not required for processing when the data is available from sources accessible to the general public.

[81] Article 2 of the LOPD.

[82] Article 8 2 of the Implementing Regulation of the LOPD.



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 third exception to the need for consent from data subjects for the communication of data relates to the necessary development of legal relationships. Article 11.2.c) on the transfer envisages that consent will not be necessary when the development, compliance and control of that legal relationship between the data controller and the data subject requires communication to third parties. Such communication will only be legitimate to the extent of the purpose justifying it.

-The fourth exception to the need for consent refers to communication to the authorities and jurisdictional entities.

-The fifth exception refers to transfers taking place between public administrations and concerns the retrospective processing of the data for historical, statistical or scientific purposes. To determine what is understood by scientific one must refer to Law 13/1986 on the development and general coordination of scientific and technological research and its implementing regulations, and regional regulations on the matter. On the matter of publicly-owned files, Article 21 contains the regulations concerning the transfer of data between public administrations. It firstly establishes that the data collected or processed by public administrations in the performance of their functions will not be communicated to other public administrations for the exercise of different competencies or matters unless the communication were to have been envisaged by the provisions on the creation of the file or by the provisions of a law of a similar rank regulating their use, or when the purposes is the retrospective processing for historical, statistical or scientific purposes. In these two instances, the rule establishes that data subject consent will not be required.

-The final exception arises when the transfer of personal data on health is necessary for resolving an emergency which requires access to a file or for conducting epidemiological studies within the terms of central or regional government health legislation. As a result, health centres and professionals will be able to process data on their patients without their consent under the terms of the aforementioned health legislation, although for their transfer their consent will be required, except in the specific instances referred to in Article 11.2 f. of Article 10.5 of the Implementing regulation of the LOPD, which states that "Specially protected data may be processed and disclosed under the terms provided in Articles 7 and 8 of Organic Law 15/1999, of 13 December.

In particular, consent of the data subject will not be required for the communication of health related personal data, including via electronic means, between bodies, centres and services of the Spanish National Health Service when it is for the purpose of medical care of persons, pursuant to the provisions of Chapter V of Law 16/2003, of 28 May, on the cohesion and quality of the Spanish National Health Service."

Section 3 of the Article considers the case that communication of the data requires the prior consent of the data subject and it is wished to ensure that such consent is granted with full knowledge of the purpose for which the data will be used, the intention of the transfer and the type of activity to be performed by the party that will be assigned the data. It states that consent for the communication of personal data to a third party will be null and void when the information given to the data subject does not enable him to know the purpose for which the data being communicated is authorised or the type of activity of the person to whom it is intended to communicate the data.

Section 6 of the Article is of particular importance, as it refers to the decoupling procedure. This is defined in Article 3.f) as any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person[83]. Article 11.6 excepts communications that have been preceded by a decoupling procedure from the provisions of the rest of the Article.

Article 27 of the LOPD regulates the communication of data transfers. In some of the instances in which the consent of the data subjects is not necessary for the ceding or communication of their data, the communication of the first transfer will be necessary, such as for example in the case of transfers authorised by law, when data has been collected from sources accessible to the public, and when the transfer of personal health data is necessary to resolve an emergency. In other cases, such as when the information is provided after a decoupling procedure and when

[83] Decoupling procedure means anonymisation process in LOPD.



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

communication is required by law, it will not be necessary to comply with the requirement to communicate this to the data subjects. In these cases it will be neither necessary to obtain the consent of the data subjects affected by the transfer nor to communicate the first transfer of data.

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

The LAP establishes in Article 16 the general rule that professionals at the centre performing the diagnosis or the treatment of the patient have access to the clinical history for healthcare purposes. Nevertheless, access for legal, epidemiological, public health, research or teaching purposes, is governed by the terms of the LOPD and the General Tax Act and remaining applicable legislation. Access for these purposes requires the personal identification data of the patient to be kept separate from the clinical care data, so that as a general rule anonymity can be assured, unless the patient were to have consented to them not being separated.

Access to the data and document of the clinical history is strictly limited to the specific purposes of each case. The administration and management personnel of the health centre will only be able to access the clinical history data related to their own functions. Duly accredited health staff performing inspection, evaluation, accreditation and planning tasks can have access to clinical records as part of as part of their duty to verify the quality of assistance, the observance of patient rights or any other of the centre's obligations in relation to its patients or users or the administration of health services itself.

As a complementary guarantee of patient privacy it is stated that access to their data on clinical records will be strictly restricted to the specific purposes of each case, which is no more that application of the principle of proportionality (disregard for privacy is justified when necessary to attend to another legitimate purpose, such as research in this case). Thus, the medical data on the clinical records will be able to be used for the purposes of Article 16.3 of the LAP (legal, epidemiological, public health, research or teaching purposes) but always ensuring adequate confidentiality that guarantees that only those patients who have provided their consent for the purpose will become known.

Health data on the clinical records of a patient will only be able to be communicated to another professional if the latter is to carry out treatment or diagnosis of the patient in question, or if the patient were to request the transfer of the medical records to another physician, notwithstanding the duty to preserve the previous record (Report 381/2003 and 488/2004).

**The LIB** regulates in a general manner the necessary express, written consent of the data subject in the case of the ceding of personal data to third parties unrelated to medical healthcare or biomedical research. If the data reveal information on family members, the assignment will require the written consent of all the data subjects[84].

In the case of genetic data of a personal nature, the LIB establishes that written consent should be obtained from the source data subject. This represents a variation with regard to the LOPD, which contemplates an exception to the express consent if the treatment is necessary for medical prevention or diagnosis or the administration of health services. It could be understood that it would be sufficient for the prior consent to also agree to the processing of their data without the need for separate, specific consent to be given on the matter of data protection. This is not

[84] Article 5 of the LIB.



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 case however with genetic data, for which express written consent must be obtained with regard to personal data.

The same situation exists with regard to the ceding of data for research purposes. The law establishes that data may only be used for purposes of research, public health and teaching when the data subject has provided consent or when it has first been made anonymous. The only exception is when in exceptional circumstance in the general health interest the competent authority, having received a favourable opinion from the data protection authority, will be able to authorise the use of genetic or codified data, always ensuring that it will not be able to be linked to the source data subject by third parties[85].

The system for the conservation, use and ceding of biological samples is the subject of detailed regulation. In relation to the dilemma as to the possibility of either granting a completely generic consent or specific consent for the use or subsequent uses of the sample, the law has opted for an intermediate, flexible regime whereby initial consent may cover subsequent research related to the initial research, including research that may be carried out by third parties and the transfer to them of data or samples that are either identified or identifiable. In any case, a transitory regime has been envisaged regarding those biological samples obtained for any purpose prior to the coming into force of this Law so as not to hinder their use for research, at the same time as protecting the interests of the source data subjects[86].

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

According to the study, data processing must be based on a series of principles: quality, consent, duty to inform, the principle of security and the duty to secrecy.

The basic principle is that of data quality, according to which data will only be able to be used for purposes compatible with those for which they were collected, and must be erased once they cease to be pertinent and necessary for such purposes. Nevertheless, an exception to the general regime is envisaged, regulated in Chapter VII, Title IX of the Implementing Regulation of the LOPD, according to which data may be retained for processing for historical, statistical or scientific purposes.

In addition, the principle of consent requires consent to be obtained from data subjects for the processing of their personal data. In the case of health data, data subjects can count on the additional guarantee envisaged by Article 7 of the LOPD, which is that consent for the processing of such data must be expressly stated.

In the case of the duty to inform regulated in Article 5 of the LOPD, this gives way in those cases when waived by law, when the processing is for historical, statistical or scientific purposes, or when the information is impossible to obtain or requires a disproportionate effort in the opinion of the AEPD.

Lastly, the data subjects will be able to claim their ARCO rights (the right to access, rectify, suppress and oppose their data).

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

As mentioned previously, the LAP establishes certain guarantees for data subjects whose data is processed for research purposes. In first place, in the case of access for research purposes, personal identification data must be

[85] Article 3.k (coded data or pseudonymised data).

[86] Articles 58 and 60 of the LIB.



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

kept separate from healthcare data, so that anonymity can be assured. Nevertheless, it is possible for the patient to consent to them not being separated. In that way it can be guaranteed that access to clinical records is restricted to the specific purposes of each case, and thus that the principle of proportionality is respected, so that only the data of patients who have granted their consent becomes known.

In addition, data are required to be kept in secure conditions for at least 5 years. The patient has the right to ensure that the centres have established an active and diligent mechanism for the safeguarding of their data. Lastly, data may only be ceded to another professional if the patient has requested their transfer to another medical professional.

The LIB lays down the requirement for express, written consent from the data subject when personal data is to be transferred to third parties. In addition, it contemplates an additional safeguard with regard to the LOPD in the case of the treatment of genetic data of a personal nature, which is that consent in addition to being express, must be in writing. In the case of the ceding of data for research purposes, this will only take place after a report has been obtained from the data protection authority and as long as it is ensured that the data is anonymised, in other words, that it cannot be linked to the source data subject by third parties[87].

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

## 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?

Article 9 of the LOPD establishes a general rule prohibiting processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Its second section establishes several exceptions. These include Article 9.2 j) of the GDPR that allows processing when it "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 will 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."

[87]Article 50.2 LIB. Likewise, article 5.2 LIB confirm this by saying "personal data transfer to third parties to biomedical research, shall require the data subject´s explicit and written consent". Article 51.1 establishes that.



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

Implementation of this article in Spain can be found in Article 9 of the Bill. In the first place, it modifies the prohibition on the processing of sensitive data. The law enables the processing of sensitive data under the terms of the exceptions of Article 9.2, except for the one established in Article 9.2.a) of the GDPR. The bill makes no statement in relation to section 9 j) of the GDPR. In its second section it establishes that the law may approve the processing of health data in the health field when so required by the administration of health and social assistance systems and services, whether public or private.

On the matter of recent developments in relation to the processing of health data, the fact is that the new developments are to be found in the GDPR itself, and this is because as indicated in the Ninth Additional Provision of the Draft Bill, the Government will within a term of two years as from the coming into force of this organic law send to Parliament a bill in which it will establish additional conditions, and if necessary, restrictions, on the processing of genetic, biometric or health-related data. For this reason, in the interim we must refer to the GDPR to determine the first new developments introduced in relation to the healthcare field. First, we must highlight two of its definitions in its articles, such as the definitions of "data concerning health" and "genetic data." In the case of the first of these, the regulation incorporates a novel aspect to the traditional concept of health-related data, as it also includes under this definition information or data in relation to the provision of health care services that reveal information on a person's health status. They are also included in the definition of genetic data.

In second place, on the matter of the lawfulness of the processing of what it defines as sensitive data, this lawfulness is restricted to the fact that the data subject should have granted explicit consent, or that processing should be necessary for preventive medicine, medical diagnosis, the providing of healthcare or treatment, as well as for the management of healthcare systems and services. Nevertheless, such processing is conditional on its being performed by a professional bound by professional secrecy laws.

Similarly, note should be made of the reference in the GDPR to the processing of persona data for the purposes of scientific research and its requirements. Personal data must be collected for a specific, explicit purpose, and will not be able to be used subsequently in a manner incompatible with such purpose. Nevertheless, the Regulation states that its subsequent processing for scientific purposes will not be incompatible, adding that in the case of sensitive data (health data) processing must be authorised explicitly by the data subject, or it should be necessary to pursue scientific research purposes. However in recital 33 to the GDPR a series of obligations are listed: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

Therefore, it limits the exercise of consent by data subjects whose data are going to be used subsequently for purposes of scientific research, restricting it solely to certain areas of research or parts of a project. Nevertheless, nothing further is specified, with Member States being responsible for its interpretation.

The Bill plans for its regulatory development to take place by means of a Royal Decree.

On the matter of the regulation of the sector, special attention should be paid to the AEPD report on the influence of the GDPR on the current regulatory framework in force in Spain in relation to the processing of data for biomedical research. According to the latter, current regulations for the healthcare sector will not be changed and will be maintained.



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 regulations are based on the approval for the processing of health data of Article 7.3 of the LOPD when provided for by law or the data subject has given explicit consent. Article 58 of the LIB requires the consent of the data subject for the use of human biological samples for the purpose of biomedical research. On the matter of possible secondary use, the law takes consent as an essential basis for processing, whether or not the data is made anonymous. Nevertheless, an exception is made when it is not possible to obtain consent, or it represents an unreasonable effort. In this regard it should be considered whether the research is in the public interest, whether it is carried out by the same institution, if there is any express objection from the data subject, if the confidentiality of the personal data is ensured, etc. This rule is complemented by Article 60 of the LIB, which relaxes the criterion in the case of the use of the data in secondary research.

Therefore, the model on the matter of biomedical research is based on the consent of the source data subject, which may be waived if it is not possible to identify the subject because of anonymisation of their data, or when research is considered to be compatible with the initial research. Except in these cases, according to the law it will be necessary for the express consent of the data subject (Article 58.2) for specific research (Article 60.1).

On the matter of data in relation to health, Article 9.1 of the GDPR is based on the general principle of prohibition of processing. Nevertheless, an exception to this principle is made in the cases listed in Article 9.2 that authorise processing in certain cases. Specifically "when 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 will 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."

In addition, on the matter of the limitation of the purpose, Article 5.1 b) of the GDPR establishes that "in accordance with Article 89 section 1, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes."

The contentious issue with regard to Spanish regulations concerns the possible secondary use of healthcare data. The GDPR establishes that in the case of different purposes consent must be granted for each one. This implies that those cases where processing is based on consent, the data subject must be clearly and unequivocally aware of the purposes for which the process will be carried out. Nevertheless, this is only applicable when consent is the legal basis for the processing and not for those cases in which the law authorises processing, such as happens for example in Article 58 of the LIB.

In its recital 52, the GDPR itself states that exceptions to the prohibition on processing special categories of personal data "should be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular (…) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes," and the first clause of recital 53 adds that "special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole," again referring to the processing of data for scientific research purposes.

From all this it can be determined that the requirements for specificity and unequivocal nature for the granting of consent must not be interpreted restrictively within the sphere of scientific research, or limited to specific research for which all available information is to be provided, as it should be considered that these requirements are present in cases in which consent is granted in a given field of research, with such consent being able to be extended in future, without this in any way invalidating it, even in the case of "purposes" or areas of research that could not even have been contemplated at the time consent was granted.



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 AEPD concludes that the GDPR and the LOPD Bill not only keep the regime contained in the regulations on biomedical research unchanged, they also enable a more flexible interpretation of the scope that may be given to the consent that has been provided.

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

The GDPR envisages the obligation to carry out an impact assessment on data protection in certain cases. In particular, Article 35.3. b) refers to the processing on a large scale of special categories of data referred to in Article 9, which include health-related data.

This assessment will contain at least a systematic description of the envisaged processing operations and the purposes of the processing; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address the risks.

If the impact assessment were to reveal a high risk, the controller must consult the control authority. If this authority considers that the processing could infringe the GDPR, it will have a term of 8 weeks from the consultation to advise the controller, and if necessary the processor, in writing.

Nevertheless, section 5 of Article 36 allows Member State law to require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Article 28 of the Bill establishes that data controllers and processors will determine the appropriate technical and organisational measures they must apply to guarantee and demonstrate that processing is in accordance with the regulation. In particular, they will determine whether it will be necessary to perform an impact assessment regarding the data protection or make a prior consultation as per Article 36 of the GDPR.

Furthermore, the providing of incorrect information to the data protection authority in the event of the submission of a prior consultation will be deemed a minor infringement.

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

The GDPR comes into effect on 25 May 2018, and as a result, the first of the obligations of data controllers handling personal data comes to an end: the free of charge notification of files to the General Data Protection Register of the AEPD. The implementation of the new General Data Protection Regulation as from 25 May 2018 imposes different obligations on the matter of data protection. Article 30 stipulates that each controller and, where applicable, the controller's representative, will maintain a record of processing activities under its responsibility. The controller is therefore once again faced by the need to describe what data are collected, for what purpose they are processed, to whom they are communicated, whether they are transferred to other countries, what technical and organisational measures will be applied to safeguard them, and when it will be able to eliminate them.



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

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

Article 89 of the GDPR provides for derogation from the right of the data subject to access the data, the right to rectification and the limitation of their purpose. Nevertheless, these measures will only apply if those rights make it impossible or seriously impair the achievement of the scientific purposes that are the object of the processing.

The Bill does not make specific reference to the processing of specially protected data for research purposes. Therefore, the provisions regarding consent, information, etc. of the Bill will apply.

## 5. Further processing for research purposes under the GDPR

### The notion of further processing under the GDPR:

Article 5 of the GDPR regulates the principles relating to processing of personal data. Section 1 b) establishes that personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Therefore, further processing for a purpose compatible with that for which collected will be legitimate, without the need to again obtain consent.

### How to measure the compatibility of purpose of the further processing:

Where the processing is for a purpose other than that for which the personal data have been collected, according to Article 6.4 of the GDPR the controller must take a series of elements into account. This "test for verification of the compatibility of a purpose other than that justifying the data gathering" considers various aspects.

In the first place, any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; the nature of the personal data, in particular whether special categories of personal data are processed; the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the result of the test is positive, and none of the elements makes any further processing unlawful, no legal approval is required for subsequent processing. If not, this further processing will require independent legal approval.

### The particularities of scientific research: a presumption of purpose compatibility

However, the processing for scientific research purpose is an exception. Indeed, under Article 5 (1) (b) of the GDPR the compatibility of the processing purpose of further processing with the initial purpose of the collection is presumed under Article 89 (1). Here the GDPR establishes a presumption of compatibility of purposes for scientific research purposes. The reasoning behind this exception can be easily imagined. Scientific research is very often based on existing data, this is why allowing the processing of personal data for different (if not incompatible) purposes is fundamental for scientific research.

This assumption made for the benefit of scientific research is linked to the derogation of the principle of data minimisation for scientific research purposes. However, this presumption is limited by some requirements, which are set out in Article 89(1) of the GDPR: the appropriate safeguards for the data subject's rights and freedoms, and



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

ensured technical and organisational measures, such as pseudonymisation. Although a different scenario would require different technical and organisational measures to ensure the safeguards for the data subject's rights and freedoms. This is clearly indicated in recital 156 of the GDPR: "The further processing of personal data for (…) scientific (…) research purposes (…) is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which does not permit or no longer permits the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data)."

Additionally, further processing of personal data is connected to the principle of storage limitation (Article 5(1)(e) of the GDPR), as it also constitutes a derogation to that principle, "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject".

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

GDPR rules are applicable directly. As a result, the Bill makes no reference to compatible purposes and the requirements they must meet.

As described previously, the LOPD does not consider further processing for historical, statistical or scientific purposes to be incompatible. Furthermore, based on their historical, scientific or statistical value these data may be maintained according to specific legislation. This procedure, contemplated in Article 4.5 of the LOPD, is developed in the implementing regulation of the LOPD.

As a result, these references and the compatibility of processing of data for a purpose other than that for which collected are eliminated.

# 6. Health data sources for research purposes

## a. Sources of data and their regulation

***Does your national framework contain specific provisions for anonymised or pseudonymised health data?***

To establish that proper anonymization is performed it is necessary to refer to the definition of Article 3 f) of the LOPD that considers it to be "any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person."

This concept is repeated in Article 5 of the Implementing Regulation of the LOPD, which in Article 5.p) defines the decoupling procedure as "any data processing allowing dissociated data to be obtained." In section e) it specifies that decoupled data is "that not allowing identification of the data subject".



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

Decoupling implies the anonymization of personal data, with the loss of all links to the individual owner of the personal data. As decoupled data do not have any direct or indirect link to an identified or identifiable person they do not fall within the scope of application of the LOPD, as they cannot be considered to be data of a personal nature.

Use of this procedure prior to the access to and processing of the data enables the data to be exempted from compliance with the obligations established by the LOPD. For example, it allows such data to be communicated without the need to obtain prior consent from the data subject[88].

In the case of specific regulation on the health sector, the LAP allows access to clinical histories, and in addition to its use for healthcare purposes it may be used for epidemiological purposes, public health, research and teaching. In these cases the law provides two alternatives: either consent can be obtained from the patient, or the information can be disassociated, that is to say, the personal information and the clinical healthcare information are kept separate.

On the matter of genetic analyses, the LIB establishes that such analyses may only be carried out for healthcare purposes and biomedical research, any commercial use of such analyses being prohibited. Before genetic analysis is performed a duty to inform must be fulfilled regarding the proposed use and purpose of the results, as well as its implications for the data subject and other family members, and written consent must be obtained from the interested party.

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

- **DIRECT COLLECTION FROM 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.

Health data are considered to be especially protected, and processing will only be authorised when provided for in law for reasons of public interest or because the data subject has given express consent to it.

Nevertheless, personal health data will be able to be processed when such processing is necessary for medical prevention or diagnosis or the administration of health services, as long as it is performed by a healthcare professional bound by the duty of secrecy. Such data may also be processed when necessary to safeguard the vital interests of the data subject.

It is therefore necessary to comply with rules on informed consent and the duty to inform. Article 5 establishes the duty to inform the data subjects in advance of the existence of the file, and whether their replies are mandatory or optional, the consequences of the obtaining of the data, the possibility of their exercising their ARCO rights, and the identity and address of the data controller.

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

[88] Article 11.6 of the LOPD.



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

Additional Provision Nine of the Draft Bill establishes that the processing of health data will be subject of regulation within two years. Therefore, the legal framework established by the GDPR is to be applied.

- **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.**

As a general rule, Article 7.3 of the LOPD establishes that "personal data that refer to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his explicit consent." This article establishes the essential content of the fundamental right to personal data protection because of its organic nature.

The special protection granted to personal health data is not arbitrary, as it derives from the terms of international and community rules regulating the automated processing of personal data. In this context, Article 8 of Directive 95/46 refers to health data as being subject to special protection. Article 8 of the Directive restricts the processing of data to specific instances and purposes for which express consent will be required from the data subject, or to when processing is required for healthcare purposes or to protect the vital interests of the data subject.

Article 7.3 having established the general rule requiring consent for the processing of health data, Article 7.6 establishes in its first paragraph that "the personal data referred to in paragraphs 2 and 3 of this Article may be processed when such processing is necessary for purpose of preventive medicine or diagnosis, the provision of medical care or treatment, or the management of health-care services, provided such data processing is effected by a health professional subject to professional secrecy or by another person also subject to an equivalent obligation of secrecy."

Also, further to the second paragraph of that same Article 7.6, "The data referred to in the preceding subparagraph may also be processed when this is necessary to safeguard the vital interests of the data subject or another person in the event that the data subject is physically or legally incapable of giving his consent."

Regarding the terms of Article 7.6, document WP131 of the Group created by Article 29 of Directive 95/46/EC points out that "As Article 8(3) of the Directive is an exception from the general prohibition on processing sensitive data, this exemption must be interpreted in a restrictive way." It goes on to say that: "This derogation only covers processing of personal data for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these healthcare services, e.g. invoicing, accounting or statistics."

It does not cover further processing which is not required for the direct provision of such services, However, this legal exemption to Article 7.6, as well as to Article 8 of Organic Law 15/1999, refers to data processing, not its assignment.

In addition, in the context of healthcare, Article 8 adds that: "Without prejudice to the provisions of Article 11 on assignment, public and private health-care institutions and centres and the corresponding professionals may process personal data relating to the health of persons consulting them or admitted to them for treatment, in accordance with the provisions of the central or regional government legislation on health care." In this regard it is also established in Article 10.5 of Royal Decree 1720/2007 of 21 December approving the Implementing Regulation of Organic law 15/1999 that "specially protected data may be processed and disclosed under the terms laid down in Article 7 and 8 of Organic Law 15/1999 of 13 December.



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

In particular, consent of the data subject will not be required for the communication of health related personal data, including via electronic means, between bodies, centres and services of the Spanish National Health Service when it is for the purpose of medical care of the persons, pursuant to the provisions of Chapter V of Act 16/2003, of 28 May, on the cohesion and quality of the Spanish National Health Service."

In conclusion, the general rule for the collection and processing of health data requires the freely given, unequivocal, informed and express consent of the data subjects, regardless of the terms of state and regional government regulations on the matter of clinical records.

In the case of state regulations, the only law applicable to its processing and/or assignment is the LAP. This law establishes a specific regime limiting the application of the LOPD in this case, so that the accesses to clinical histories must be those envisaged in its Article 16, contemplated as the application of the exemption to consent envisaged in Article 7.3 of the LOPD.

Article 16 of the LAP restricts the instances of clinical record data assignment to third parties unrelated to the healthcare to two cases. On the one hand, access to the clinical history for legal, epidemiological, public health, research or teaching purposes that requires keeping the personal patient identification details separate from those of the healthcare data, so that as a general rule, anonymity is assured, barring express patient consent. On the other hand, personnel performing tasks for inspection, evaluation, verification and planning purposes will have access to the clinical records for the fulfilment of their duties.

In general the gathering and processing of data must observe the general principles on data protection contained in Article 4 of the LOPD that states in section 1 "Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained." Section 2 indicates that "Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected."

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

Additional Provision Nine of the Draft Bill establishes that the processing of health data will be subject of regulation within two years. Therefore, the legal framework established by the GDPR is to be applied.

- **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.

There is no specific provision regarding the creation of files with health data for research purposes. However, Article 39 of the LOPD establishes the mandatory registration of certain databases with the General Data Protection Register.

Privately-owned files containing personal data may be created when they are necessary for the business or legitimate activity of the person, company or entity owning them, and the safeguards laid down in the LOPD are observed.

Files of the public administrations may only be created, modified or deleted by means of a general provision published in the Official State Gazette or in the corresponding official journal (article 20.1 of the LOPD)



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

Before generating databases for the storing of health data, their owners must define and document their structure, the type of documents intended to be gathered, the procedure for collecting the data, the purpose for which the database has been created, the uses to be given to it, the assignments planned for the data stored, the security measures to be adopted regarding its content and the name of the persons and bodies responsible for its use. These specifications must been informed to the Spanish Data Protection Agency and recorded on its General Data Protection Register in the manner indicated in the regulations.

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

- **PUBLIC DATABASES**

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

In the case of public administration databases, Spanish legislation establishes that such requirements should be stated in a general provision published in the Official State Gazette or in the corresponding Official Journal.

The owners of the abovementioned databases and the medical healthcare professionals must ensure the safeguarding of the data they hold, establishing the method for the updating of the data and maintaining secrecy on data considered to be especially sensitive.

Once the prior requirements have been met, the databases will be able to be used solely for the gathering of health data that is adequate, pertinent and necessary in relation to the specific purpose of the database, which must be in accordance with the activity or legitimate purpose of its owner. Collection of data using fraudulent, misleading or unlawful means is prohibited, and the data controller will be responsible for controlling it truthfulness and accuracy and for keeping the data updated, completing and replacing such data as is incomplete or incorrect and eliminating data that is no longer necessary.

Those creating automated health-related files are also required to obtain the prior flawless consent of patients and related persons in relation to the processing of their personal data for the purpose envisaged, and they must alert data subjects to the possibility of their data being ceded to identified or identifiable third parties, except in those case when such obligation is legally waived (processing of data for the exercise of the functions of public administrations in their spheres of competence, or of data on persons linked by a legal relationship that may be necessary for maintaining or complying with such a relationship).

To ensure freedom in the granting or rejecting of such consent, healthcare personnel must provide sufficient information to the persons concerned on the existence of the file and their right to know the purpose pursued with its creation, the possible addressees of the information stored on the file and the name and address of the owner of the file. In addition, they must be informed on their right of access to their own data stored on the files and be able to correct or suppress it when appropriate.

Data obtained by healthcare personnel must be used exclusively for the intended purpose, its use, ceding or even conservation for a purpose other than that originally stipulated being prohibited.

When the owner of the file entrusts its production to third parties outside the scope of its management or organisational authority, the corresponding contractual relationship between them must detail the procedure and type of data to be gathered, the purpose of the gathering and the reciprocal obligations of the contracting parties, it being advisable to precisely specify the obligation to maintain professional secrecy regarding the data obtained, an obligation that will persist even after the end of the contractual relationship.



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 owner of the file will assume the obligations related to its content, being responsible for the licit nature of the compiling of the data, their accuracy, updating, adequacy and pertinence, the obtaining of consent from the persons affected and compliance with administrative procedures for the notifying and registration of the file on the corresponding Register, and the distributor will be responsible for the obligations related to the management of the file, control of access to it by those persons authorised to use it, informing the persons concerned about the first assignment of their data, as well as the security of the file, its logical and physical supports used for its processing and storage, and the place where the file is located.

Those receiving the information containing health data processed automatically must only use it for purposes in accordance with the legitimate aims of the file owner, with the legislation regulating the automated processing of data being applicable to any subsequent use, even if not automated, that the receiving parties may make of such data, assuming in the event of subsequent assignments of the information the role of producers or distributors of personal data, with the legal requirements applicable to them.

Legislation on the regulation of the automated treatment of personal data envisages the possibility of reaching sectoral accords or business agreements for the formulation of standard codes of an ethical nature circumscribed to the sector of the agreement that establish general conditions, obligations, rights and safeguards to be demanded from those involved in the processing and automated use of personal information. These codes should be mandatorily supervised by the Spanish Data Protection Agency.

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

No.

## b. Application of the national framework to the AEGLE cases

AEGLE is a European project funded through the Horizon 2020 framework programme that has brought together thirteen organizations with interdisciplinary backgrounds, from academia, the technological and engineering sciences, to the medical, legal and ethical areas, to create and build an innovative ICT solution for Big Data management in the healthcare sector. This solution will revolutionise integrated and personalised healthcare services.

The AEGLE project aims to overcome these difficulties and generate value from healthcare data through the development of a framework for Big Data analytics that will improve translational medicine, to facilitate personalized and integrated care services, and to promote data-driven research across Europe.

The data generated in the health domain is coming from heterogeneous, multi-modal, multi-lingual, dynamic and fast evolving medical technologies. AEGLE will:

-Realize a multiparametric platform using algorithms to analyze big biodata including features such as volume properties, communication metrics and bottlenecks, estimation of related computational resources needed, handling data versatility and managing velocity



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

-Address the systemic health big bio-data in terms of the 3V multidimensional space, using analytics based on PCA techniques

-Demonstrate AEGLE's efficiency through the provision of aggregated services covering the 3V space of big bio-data. Specifically it will be evaluated in: a)big biostreams where the decision speed is critical and needs non-linear and multi-parametric estimators for clinical decision support within limited time, b)big-data from non-malignant diseases where the need for NGS and molecular data analytics requires the combination of cloud located resources, coupled with local demands for data and visualization, and finally c)big-data from chronic diseases including EHRs and medication, with needs for quantified estimates of important clinical parameters, semantics' extraction and regulatory issues for integrated care

- Bring together all related stakeholders, leading to integration with existing open databases, increasing the speed of AEGLE adaptation.

- Build a business ecosystem for the wider exploitation and targeting on cross-border production of custom multi-lingual solutions based on AEGLE.

Currently the main implications faced during the AEGLE's progress concern ethical and legal aspects that may affect the wider addition of AEGLE, as well as the user perception regarding the use of sensitive data. Despite the common directives imposed by the EC the local (in country level) legal frameworks differ and they are quite fragmented. The anonymization techniques will enable AEGLE consortium to tackle these challenges leading to the wider adoption of the platform and the maximum exploitation of project's features.

AEGLE has chosen three medical use cases to focus the biomedical research questions and set the basis for bio-signal and bioinformatics analytics, multi-parametric pattern mining, and integrative predictive modelling. The use cases are Chronic Lymphocytic Leukemia (CLL), Intensive Care Unit (ICU) and Type 2 Diabetes (T2D).

This section aims to address each of the processes relevant to data under the Directive (the current framework) and the GDPR.

## 1. Type 2 diabetes

Diabetes Mellitus (DM) is defined as a group of metabolic disorders mainly caused by abnormal insulin secretion and/or action. Insulin deficiency results in elevated blood glucose levels (hyperglycemia) and impaired metabolism of carbohydrates, fat and proteins. DM is one of the most common endocrine disorders, affecting more than 200 million people worldwide. The onset of diabetes is estimated to rise dramatically in the upcoming years. DM can be divided into several distinct types. However, there are two major clinical types, type 1 diabetes (T1D) and type 2 diabetes (T2D), according to the etiopathology of the disorder. T2D appears to be the most common form of diabetes (90% of all diabetic patients), mainly characterized by insulin resistance. The main causes of T2D include lifestyle, physical activity, dietary habits and heredity, whereas T1D is thought to be due to autoimmunological destruction of the Langerhans islets hosting pancreatic-β cells.

The risk of developing T2D can be increased by various factors; usually a mixture of modifiable and non-modifiable elements of age, weight, genetics and ethnicity. The AEGLE system will analyse the inter dependences of the factors including medication that are known to have a detrimental effect in type 2 diabetes to give a prediction on the



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

potential deterioration. This would enable intervention to enable reduction of mortality, complications and hospitalization that would all lead to reduction in overall health costs.

The power and effectiveness of these approaches are derived from the ability of commensurate methods to extract patterns and create models from data. The aforementioned fact is particularly significant in the big data era, especially when the dataset can reach terabytes or petabytes of data. Consequently, the abundance of data has strengthened considerably data-oriented research in biology. In such a hybrid field, one of the most important research applications is prognosis and diagnosis related to human-threatening and/or life quality reducing diseases. One such disease is diabetes mellitus (DM).

Advantages for the T2D case: supports the definition of prognostic indicators; improves methods and points for intervention; supports the definition of accurate cohort and feasibility for clinical trial; allows for improved monitoring and therapeutic modalities.

For non-malignant chronic diseases, like diabetes mellitus type 2, AEGLE offers a research platform that allows clinical researchers, hospitals management and pharmaceutical organisations to analyse their own EHR data. The platform and analytics available in AEGLE platform offer users much more flexibility in deciding what to analyse and for which patient populations in the hospital to develop/use predictive analytics. The analytics included can facilitate research into pharmacovigilance, treatment response, and complications whilst the visualization tools such as heatmaps and population pyramids can be used for hypothesis generation, but also presentation of quality metrics.

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

As explained above, further treatment requires the compliance with the principle of data quality in the processing of data. Article 4 of the Law forbids the use of the data for purposes incompatible with those for which it was collected. In addition, the Implementing Resolution for the LOPD establishes that data of a personal nature may only be collected to comply with specific, explicit and legitimate purposes by the data controller. Such personal data may not be used for purposes incompatible with those for which they were collected. As It was explained, the general rule is that data should be erased once it is no longer to be used for the purpose for which it was collected. Nevertheless, there´s an exception in the case of data gathered for statistical, historical, or scientific purposes. The procedure is developed in Chapter VII of Title IX of RD 1720/2007.

The communication or assignment of data is regulated by Article 11 of the LOPD. For analysis of the legal clauses in relation to communication one must refer to the definition established in Article 3.i) of the LOPD. Thus, assignment or communication of data: any disclosure of data to a person other than the data subject. The law establishes two requirements for the validity of the assignment or communication of data: the communication must reflect compliance with the purposes directly related to the legitimate functions of the assignor and assignee, and it should furthermore count on the prior consent of the data subject.

Regarding specific sector regulation, LAP establishes in article 16 the general rule that professionals at the centre performing the diagnosis or the treatment of the patient have access to the clinical history for healthcare purposes. Nevertheless, access for legal, epidemiological, public health, research or teaching purposes, is governed by the terms of the LOPD. Access for these purposes requires the personal identification data of the patient to be kept separate from the clinical care data, so that as a general rule anonymity can be assured, unless the patient were to have consented to them not being separated.

Access to the data and document of the clinical history is strictly limited to the specific purposes of each case. Thus, the medical data on the clinical records will be able to be used for the purposes of Article 16.3 of the LAP (legal, epidemiological, public health, research or teaching purposes) but always ensuring adequate confidentiality that guarantees that only those patients who have provided their consent for the purpose will become known.



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 LIB regulates in a general manner the necessary express, written consent of the data subject in the case of the ceding of personal data to third parties unrelated to medical healthcare or biomedical research. If the data reveal information on family members, the assignment will require the written consent of all the data subjects.

In the case of genetic data of a personal nature, the LIB establishes that written consent should be obtained from the source data subject. This represents a variation with regard to the LOPD, which contemplates an exception to the express consent if the treatment is necessary for medical prevention or diagnosis or the administration of health services. It could be understood that it would be sufficient for the prior consent to also agree to the processing of their data without the need for separate, specific consent to be given on the matter of data protection. This is not the case however with genetic data, for which express written consent must be obtained with regard to personal data.

The same situation exists with regard to the ceding of data for research purposes. The law establishes that data may only be used for purposes of research, public health and teaching when the data subject has provided consent or when it has first been made anonymous. The only exception is when in exceptional circumstance in the general health interest the competent authority, having received a favourable opinion from the data protection authority, will be able to authorise the use of genetic or codified data, always ensuring that it will not be able to be linked to the source data subject by third parties.

The system for the conservation, use and ceding of biological samples is the subject of detailed regulation. In relation to the dilemma as to the possibility of either granting a completely generic consent or specific consent for the use or subsequent uses of the sample, the law has opted for an intermediate, flexible regime whereby initial consent may cover subsequent research related to the initial research, including research that may be carried out by third parties and the transfer to them of data or samples that are either identified or identifiable. In any case, a transitory regime has been envisaged regarding those biological samples obtained for any purpose prior to the coming into force of this Law so as not to hinder their use for research, at the same time as protecting the interests of the source data subjects.

**Once the GDPR has been implemented:**

GDPR rules are applicably directly. The LOPD Bill makes no references to compatible purposes and the requirements.

Article 5 of the GDPR regulates the principles relating to processing of personal data. Section 1 b) establishes that personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Therefore, further processing for a purpose compatible with that for which collected will be legitimate, without the need to again obtain consent.

Where the processing is for a purpose other than that for which the personal data have been collected, according to Article 6.4 of the GDPR the controller must take a series of elements into account. This “test for verification of the compatibility of a purpose other than that justifying the data gathering” considers various aspects. If the result of the test is positive, and none of the elements makes any further processing unlawful, no legal approval is required for subsequent processing.

However, the processing for scientific research purpose is an exception. Indeed, under Article 5 (1) (b) of the GDPR the compatibility of the processing purpose of further processing with the initial purpose of the collection is presumed under Article 89. Here the GDPR establishes a presumption of compatibility of purposes for scientific research purposes. This presumption is limited by some requirements, which are set out in Article 89 of the GDPR: the appropriate safeguards for the data subject’s rights and freedoms, and ensured technical and organisational measures, such as pseudonymisation.

So, LOPD, LIB and LAP are to be applied as well as GDPR. Therefore, according to GPDR, processing of data for research in the field of health assumes a compatible purpose. If the “test for verification of the compatibility of a



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

purpose other than that justifying the data gathering" is positive, no legal approval is required for subsequent processing. However, the requirements of article 89 GPDR must be granted. In particular, processing of health data for research purpose must ensure the rights and freedom of the data subject. The safeguards 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 the identification of the data subjects, those purpose shall be fulfilled in that manner.

Subsequently, GDPR and LOPD keep the regime contained in the regulations on biomedical research unchanged and sector-specific regulation is to be applied.

Therefore, the model on the matter of biomedical research is based on the consent of the source data subject, which may be waived if it is not possible to identify the subject because of anonimisation of their data, or when research is considered to be compatible with the initial research. Except in these cases, according to the law it will be necessary for the express consent of the data subject (Article 58.2) for specific research (Article 60.1).

On the matter of data in relation to health, Article 9.1 of the GDPR is based on the general principle of prohibition of processing. Nevertheless, an exception to this principle is made in the cases listed in Article 9.2 that authorise processing in certain cases. Specifically "when 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 will 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."

In addition, on the matter of the limitation of the purpose, Article 5.1 b) of the GDPR establishes that "in accordance with Article 89 section 1, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes."

The contentious issue with regard to Spanish regulations concerns the possible secondary use of healthcare data. The GDPR establishes that in the case of different purposes consent must be granted for each one. This implies that those cases where processing is based on consent, the data subject must be clearly and unequivocally aware of the purposes for which the process will be carried out. Nevertheless, this is only applicable when consent is the legal basis for the processing and not for those cases in which the law authorises processing, such as happens for example in Article 58 of the LIB.

In its recital 52, the GDPR itself states that exceptions to the prohibition on processing special categories of personal data "should be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular (…) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes," and the first clause of recital 53 adds that "special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole," again referring to the processing of data for scientific research purposes.

From all this it can be determined that the requirements for specificity and unequivocal nature for the granting of consent must not be interpreted restrictively within the sphere of scientific research, or limited to specific research for which all available information is to be provided, as it should be considered that these requirements are present in cases in which consent is granted in a given field of research, with such consent being able to be extended in future, without this in any way invalidating it, even in the case of "purposes" or areas of research that could not even have been contemplated at the time consent was granted.



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

## 2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient´s consent, after pseudonymisation. The operation realised in the AEGLE project qualifies as processing for research in the field of health purposes. The data is collected by health professionals in ICU services when they are treating patients.

In this case, the processing implies communication of data. Article 11 LOPD regulates the requirement for the validity of the assignment or communication of data: the communication must reflect compliance with the purposes directly related to the legitimate functions of the assignor and assignee, and it should count on the prior consent of the data subject.

Article 11.6 LOPD contains and exception for data subject´s consent. The transfer of personal data on health is necessary for resolving an emergency which requires access to a file or for conducting epidemiological studies within the terms of central or regional government health legislation. As a result, health centres and professionals will be able to process data on their patients without their consent under the terms of the aforementioned health legislation, although for their transfer their consent will be required, except in the specific instances referred to in Article 11.2 f. of Article 10.5 of the Implementing regulation of the LOPD, which states that “Specially protected data may be processed and disclosed under the terms provided in Articles 7 and 8 of Organic Law 15/1999, of 13 December.

In this case, LAP is also to be applied. As I it was explained before, article 16 establishes the general rule that professionals at the centre performing the diagnosis or the treatment of the patient have access to the clinical history for healthcare purposes. Access to the data and document of the clinical history is strictly limited to the specific purposes of each case. As a complementary guarantee of patient privacy it is stated that access to their data on clinical records will be strictly restricted to the specific purposes of each case, which is no more that application of the principle of proportionality (disregard for privacy is justified when necessary to attend to another legitimate purpose, such as research in this case). Thus, the medical data on the clinical records will be able to be used for the purposes of Article 16.3 of the LAP (legal, epidemiological, public health, research or teaching purposes) but always ensuring adequate confidentiality that guarantees that only those patients who have provided their consent for the purpose will become known.

Once the GPDR has been implemented:

Article 9 of LOPD enables the processing of sensitive data under the terms of the exceptions of article 9.2 GPDR. The Bill makes no statement in relation to data processing in the field of research. As indicates in Ninth Additional Provision of the Draft Bill, the Government will within a term of two years as from the coming into force of this organic law send to Parliament a bill In which it will establish additional conditions on the processing of genetic, biometric or health related data. For this reason, we must refer to GDPR to determine the new development introduced in healthcare field.

In the first place, article 5 GDPR regulates the principles relating to processing of personal data. Section 1 b) establishes that personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Therefore, further processing for a purpose compatible with that for which collected will be legitimate, without the need to again obtain consent.
Where the processing is for a purpose other than that for which the personal data have been collected, according to Article 6.4 of the GDPR the controller must take a series of elements into account. This “test for verification of the



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

compatibility of a purpose other than that justifying the data gathering" considers various aspects. If the result is positive, no legal approval is required for subsequent processing.

However, the processing for scientific research purpose is an exception. Under Article 5 of the GDPR the compatibility of the processing purpose of further processing with the initial purpose of the collection is presumed under Article 89. As it was explained before, presumption is limited by some requirements, which are set out in Article 89 of the GDPR.

## 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 samples and for the processing of their data but this consent was given in general and not specifically for AEGLE.

The operation realised in the AEGLE project qualifies as processing for research in the field of health purposes.

LIB is the applicable regulation here. This law defines and clarifies the legal status of biobanks. The law establishes a single registration system for biobanks, for whatever purpose, including clinical use in patients and research purposes. The authorisation concerns to the competent body of the Autonomous Community or to the Ministry of Health and Consumer Affairs.

Article 69 establishes that the samples stored at the biobank shall be transferred for research purposes free of charge. Biological samples of human origin may only be transferred to scientifically approved research projects with Ethic and scientific committee's favourable report.

Moreover, the Act states that clinical care data could be transferred with the biological samples, in which case data protection regulation and Basic law regulating patient autonomy and rights and basic law on patient autonomy (LAP) are to be applied.

Once the GDPR has been implemented:

On the matter of recent developments in relation to the processing of health data, the fact is that the new developments are to be found in the GDPR itself, and this is because as indicated in the Ninth Additional Provision of the Draft Bill, the Government will within a term of two years as from the coming into force of this organic law send to Parliament a bill in which it will establish additional conditions, and if necessary, restrictions, on the processing of genetic, biometric or health-related data. For this reason, in the interim we must refer to the GDPR to determine the first new developments introduced in relation to the healthcare field.

Moreover, GDPR and LOPD Bill keep the regime contained in the regulations on biomedical research unchanged and enable a more flexible interpretation of the scope that may be given to the consent that has been provided.



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