# AEGLE

An Analytics Framework for Integrated and Personalized Healthcare Services in Europe

# Legal Assessment

## 'BIG DATA' ANALYTICS AND THE PROCESSING OF HEALTH DATA FOR SCIENTIFIC RESEARCH PURPOSES

| | |
|---|---|
| **DOCUMENT IDENTIFIER:** | **D7.1 – Legal Assessment** |
| **DUE DATE:** | 31/08/2018 |
| **DELIVERY DATE:** | 29/08/2018 |
| **CLASSIFICATION:** | Public |
| **EDITORS:** | Mahault PIECHAUD-BOURA,<br>Jos DUMORTIER |
| **DOCUMENT VERSION:** | 0.3 |

| | |
|---|---|
| **CONTRACT START DATE:** | 1st March 2015 |
| **CONTRACT DURATION:** | 42 months |

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

(Page intentionally blank)



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

| CONTRIBUTORS | |
|---|---|
| **Name** | **Organization** |
| Mahault Piéchaud | time.lex |
| Jos Dumortier | time.lex |
| | |
| | |
| | |
| | |
| | |

| PEER REVIEWERS | |
|---|---|
| **Name** | **Organization** |
| Arun Rattan | - |
| Barbara Pierscionek | NTU |
| John Rumbold | NTU |
| Richard Rosenquist Brandell | Karolinska Institutet |

| REVISION HISTORY | | |
|---|---|---|
| **Version** | **Date** | **Modifications** |
| 0.2 | 27/07/2018 | English language review |
| 0.3 | 28/08/2018 | Inclusions of reviewers comments |
| | | |
| | | |
| | | |
| | | |



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

# Executive Summary

During the AEGLE Innovation Action, a framework incorporating health-specific Big Data analytics combined with generic and scalable analytics was designed to generate value from the healthcare data value chain with the aim of improving translational medicine[1] and facilitating personalised and integrated care services via data-driven research. A legal assessment has been performed to determine which legal rules apply in the EU to researchers wishing to use or re-use health data for research purposes.

During the project, the European rules applying to data protection changed. Moreover, the processing of data and personal data for scientific research in the health field implies that a variety of fields of law may be relevant and apply. To have a comprehensive view of the norms applying to data processing for scientific purposes in the health field throughout the EU, this legal assessment has been based on country-specific reports collected by experts based in the different EU Member States. The results of this legal assessment are presented here.

In principle, data concerning health, but also genetic data, cannot be processed.[2] This principle was set out in the Directive and is still valid under the GDPR. There is a general prohibition on processing due to the nature of such data, as it is particularly sensitive and requires a higher degree of protection. However, a limited number of exceptions to this principle exist, such as when data subjects give their explicit consent to the processing, or when such data is processed for scientific research purposes.

Under the Directive, the processing of health data for scientific research purposes was not explicitly set out as an exception to the general prohibition on processing. Primary and further processing of health data for scientific research purposes was organised by national legislation with the implementation of suitable safeguards. In the situation of re-use of data, the Directive set up a basic regime where processing for scientific research purposes was presumed compatible with the aim of the initial processing, thus ensuring fair and lawful processing. Furthermore, while the Directive provided rights to data subjects derogations were possible for scientific research. This basic regime was often extended when the Directive was transposed into the Member States' national legal frameworks. As a result, the applicable regime was not uniform throughout the EU. The legal grounds applying to scientific research varied, as did the safeguards and modalities of processing. Despite these disparities between Member States, re-use of data without the data subject's consent was possible in most European countries. However, few Member States provided derogations to data subjects' rights for scientific research. Furthermore, the safeguards implemented varied a lot, effectively ensuring different regimes in practice. Nevertheless, some safeguards were present in many Member States, such as professional secrecy, encryption, vetting by an ethics committee etc. In some Member States, legally constituted ethics committees could demand consent before approving a scientific project. While founded upon a common base, the regime applying to the processing of personal data for scientific research purposes varied between Member States to a certain extent.

Under the GDPR, the principle applying to processing set out under the Directive continues to apply; however, from now on: the list of legal grounds is exhaustive, the data subjects' rights are more defined and so are the rules concerning the re-use of data, additionally the principle of accountability of the controller has become a 'pillar' of the system. For researchers to benefit from the scientific research regime set out in the GDPR, compliance with

[1] «translational medicine" is an inter-disciplinary field of medical science aiming to bring research results to applied medicine for new therapies and medical procedures. Definition adapted from the definition of *Science Translational Medicine*, http://www.sciencemag.org/site/marketing/stm/definition.xhtml (02/08/2018)

[2] Article 8(1) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such personal data (hereafter "DPD" or the "Directive"), and Article 9(1) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data ( hereafter "GDPR")



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

suitable safeguards is absolutely necessary. Appropriate safeguards are the new cornerstone of the regime applying to scientific research; many of them are the consequence of the application of the GDPR's general regime, but some are emphasised for scientific research, such as pseudonymisation. Moreover, Member States have provided additional requirements and safeguards in their implementation of the GDPR's open clauses. The means and the degree of further legislation are different between the Member States. Although most Member States have permitted processing for scientific research, exceptions remain, and discrepancies can still be observed. The GDPR provides the opportunity for derogations of some data subjects' rights, when exercising those rights would significantly and negatively impact upon a research project. In practice, data subjects' rights are not the same in all the Member States, and so it is the same for the applicable safeguards. These are points to which sponsors of European-wide research projects must pay particular attention.

When preparing and leading a research project based on the processing of personal data, researchers must pay particular attention to the determination of the purposes and modalities of processing, taking into account the principle of privacy by design and by default. A Data Protection Officer might have to be appointed, and processors recruited; this need means the use of a data analytics platform must be determined early on. Moreover, a record of the processing activities must be kept, and a Data Processing Impact Assessment performed. Security measures must be designed and implemented to comply with the safeguards set out at both the European and national levels. Compliance with national safeguards is a crucial and potentially problematic aspect of a transnational research project.

This legal assessment aims to establish the European framework and to indicate the areas in which European project sponsors and researchers should pay particular attention legislation applying to data protection. In doing so, a European framework applicable to scientific research was identified. This framework must be filled with national requirements in a case by case basis, depending on the modalities and scope of the processing. In its last section, the legal assessment indicates the key elements to take into consideration.



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

# Table of 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. Introduction

AEGLE is an Innovation Action that aims to generate value from the healthcare data value chain with the vision of improving translational medicine and facilitating personalised and integrated care services via data-driven research. The term 'research' here is understood in a wide sense to include applied research in the field of medicine in order to provide decision support solutions. AEGLE promotes Big Data analytics as an enabler technology platform for improving healthcare at all levels. AEGLE provides a framework incorporating health-specific big data analytics combined with generic and scalable analytics. The three use cases (CLL[3] focusing on clinical data and bioinformatics, ICU[4] with clinical and streaming data, and Diabetes with longitudinal electronic health records) cover a wide range of requirements and healthcare research expertise for the development of the AEGLE system and the testing of its value.

To conduct these three use cases, the AEGLE research team has used real medical data that has been obtained from patients in a clinical context. The data was made available to AEGLE by hospitals in Greece, Italy, Sweden and the United Kingdom. Before the AEGLE development team obtained any access to this data, it was "pseudonymised". This means that all the identifying items, such as names, addresses, dates, patients' national identification number etc., were stripped from the patient file and substituted by a code. This procedure has allowed the research team to link together data from different sources that concern the same patient but without the patient's identity being revealed.

For most of the data processed in the AEGLE framework, the patients gave their informed consent about the further use of their medical data for research purposes. This consent was not strictly necessary since European and national data protection legislation states that further processing of personal data for research purposes is presumed to be compatible with the purpose for which such data has initially been collected. However, this presumption is only valid under conditions that are determined by national law. This is the reason why different procedures are applied in AEGLE for each of the four countries from which the medical data originates. Conversely, in all the countries involved, the research performed in the context of AEGLE, and in particular the (re-)use of clinical data for this research, requires the approval of an Ethics committee, as well as the consent of data subject or the authorisation of the competent data protection authority, or the data processed must be anonymised. The procedures for obtaining such an approval vary greatly between each country.[5]

These formalities, which were completed at the project's start, demonstrated a certain heterogeneity in the different regimes, despite the common European rules for the processing of personal data. It was observed that the rules were particularly different for the reuse of data without the data subjects' informed consent.

Additionally, in April 2016 the General Data Protection Regulation (GDPR) was adopted. This new regulation lays down a revised set of rules and applies since 25 May 2018. Unlike the Directive, the Regulation is directly applicable. This should mean a fully harmonised legal framework for the processing of personal data in Europe, but the GDPR leaves no less than fifty occasions for the Member States to further legislate. These possible divergences from the general regime could have consequences for the rules applying to a data analytics platform such as AEGLE.

The GDPR's implementation has triggered the revision of national data protection legislation throughout the EU. But legislating is a slow and complicated process, in particular when the topic is as sensitive as data protection. This is

[3] Chronic Lymphocytic Leukaemia

[4] Intensive Care Unit

[5] AEGLE action, D7.2 Ethical procedures and Ethics letters.

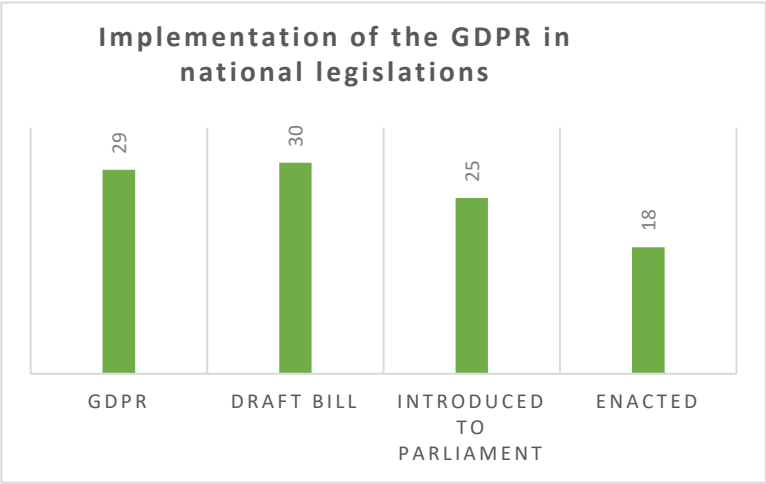


Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

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

particularly problematic for the AEGLE action. Data protection rules are integral to the success of this project, as they are most pertinent in the field of medicine and health. The GDPR takes this situation into account and leaves the opportunity for the Member States to legislate further. This is why the respective national legislations for data protection are important in the framework of this project.

However, all national legislation were not ready by 25 May 2018 when the GDPR came into force. Delays in the national legislative processes have often made the applicable legal framework difficult to assess. Figure 1 below indicates the 'state of play' concerning new national data protection legislation (22 August 2018).




| Level of implementation | Countries |
|---|---|
| GDPR | All but CH[6] |
| Draft Bill | All |
| Bill introduced to Parliament | All but EE, EL, ES, CH |
| Enacted | AT BE[7], HR, DK, FR, DE, HU, IE, LV, LU, MT, NO, PL, SK, SI, SE, NL, UK |

**Figure 1: Implementation of the GDPR in national legislation**

Data protection law affects various fields of law, and so changes may require the modifications of various legislative instruments. Moreover, in federal countries, the need to adapt applicable legislation can cover several levels of government (federal, state and local), such as is the case in Germany, where federal and State legislation has been amended to reflect the GDPR. This granularity affects the clarity of the applicable rules. This also means that modifying all the relevant legislation can take some time. This is particularly relevant for the reuse of data.

The re-use of personal data, also called the secondary use of data, was framed by high-level provisions in the Directive. These general provisions gave any Member State the power to legislate further on the matter when transposing the Directive. This legal assessment will illustrate how the Member States took this opportunity. The situation is the same under the GDPR, the provisions on the re-use of data are general, and they require compatibility with the initial processing's purpose. However, when dealing with special categories of data, any Member State can legislate further, and add more safeguards. This means that the applicable rules for the re-use of data are still likely to vary from one Member State to another.

Although the GDPR does not change much the rules applying to the re-use of data, it is not the case for the rules concerning the primary use of data. Under the Directive, the use of data for research purposes was governed mostly by national law provisions. This is no longer the case under the GDPR. The new European legislation sets out a regime applying to the processing of personal data for scientific research purposes.

[6] A table of reference for countries abbreviation can be found in annexe.

[7] In Belgium the Bill have been adopted by Parliament, but still have to be formally enacted.



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 AEGLE action is a Big Data analytics project. It is important to note that some characteristics of Big Data might be problematic in terms of data protection. Big Data is commonly defined as "*high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation*".[8] But Big Data should not be reduced to the "3Vs",[9] notably "Veracity" should be included, to address lack of accuracy. It is even argued there are different "species" of big data, and that the reference to these "3Vs" is in fact misleading.[10] The Article 29 Working Party gives a more functional definition in which "'*Big Data' refers to the exponential growth in availability and automated use of information […]. Big Data relies on the increasing ability of technology to support the collection and storage of large amounts of data, but also to analyse, understand and take advantage of the full value of data (in particular using analytics applications)*".[11]

The 'data' in Big Data does not necessarily refer to personal data.[12] For example, data produced by a ventilator, when indicting the volume of air moved is not always personal data in itself. However, it might become personal when combined with other data, such as time and location. The combination of various data sets or categories of data is one of the issues of Big Data analytics. Data, whether technical or descriptive, might become or produce personal data, due to combinations with other categories of data or processing.

This notwithstanding, Big Data remains "data" and as such subject to the rules applying to the processing of data, even, when relevant, personal data. In its report on *Big Data and Artificial Intelligence*, the ICO has identified the following aspect of Big Data analytics:[13]

- the use of algorithms
- the opacity of the processing
- the tendency to collect 'all the data'
- the repurposing of data, and
- the use of new types of data.[14]

Even with this list some aspects of Big Data analytics appear problematic for the protection of privacy and the rules applying to the processing of personal data. In the framework of the AEGLE action, the data targeted will essentially be personal data, or data, when combined with other categories of data, that could be personal data[15] (i.e. data from a ventilator, combined with a location and a time). Moreover, given the audience targeted for the platform, the data processes will contain special categories of personal data. The legal rules applying to these categories of data, such as data concerning health or genetic data, are defined both at the European and national level. A careful analysis is required to determine the scope of the applicable legal framework.

The objective of the legal assessment is to "*establish the legal issues that arise by the use of big data in health, resulting in multi-lingual and cross-border applications in Europe and worldwide. The task will define a framework*

[8] Gartner IT Glossary, https://www.gartner.com/it-glossary/big-data (04/07/2018).

[9] ICO's Guide on Big Data, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[10] Kitchin, Rob and McArdle Gavin, What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets; big Data & Society; January-June 2016; pp 1-10, p.2.

[11] Article 29 Working Party, WP 203, Opinion 03/2013 on purpose limitation, 2 April 2013, p. 45.

[12] European Data Protection Supervisor, Opinion 7/2015, Meeting the Challenges of Big Data, A call for transparency, user control, data protection by design and accountability, 19 November 2015, p.7.

[13] ICO, Guide on Big Data, artificial intelligence, machine learning and data protection; version 2.2.

[14] ICO, Guide on Big Data, artificial intelligence, machine learning and data protection, p9.

[15] Rumbold, J., Pierscionek, B., What are data? A categorization of the data sensitivity spectrum, Big Data Research ,Vol. 12, July 2018, pp. 49-59



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

*addressing these issues and will identify the parameters regarding the use Big Data in health, taking into account the national laws in the countries of AEGLE participants."*[16] In other words the core question of the legal work in AEGLE has been: what are the legal rules applying in the EU to researchers wishing to use or re-use health data for research purposes? Further, it should be noted these cannot be defined without the ethical considerations as these affect implementation of laws in medical research to varying degrees across Member states.

The establishment of a pan-European framework requires establishing what rules apply and at what level. Health and scientific research are not exclusive EU competences. This means that the framework is a combination of European and Member State level rules. Moreover, the processing of data and personal data for scientific research in the field of medicine and health implies that various fields of law[17] could be relevant and apply. First, and foremost, personal data protection law will be applied. However, the protection of privacy is not covered by a single piece of legislation and can involve decisions made in common law. Hence, the rules applying could cover various fields. For the purpose of this legal assessment, the health care and scientific research of the applying legislation have been privileged.

To determine the rules concerning the processing of special categories of data for scientific research purposes in each Member State, as well as in Norway and Switzerland, national data protection experts have been consulted. This consultation was conducted using a questionnaire[18] drafted based on a first country report (for France), and then tested on a couple of other countries, before being sent to the national experts.

The reports consistently address three (3) essential points of the processing of health data for scientific purposes:

- The **legal grounds**: the legal grounds are an important aspect of processing, as it is absolutely necessary to have all personal data processing justified by one of the reasons listed in the law. In other words: if one starts to process personal data, he/she must indicate the legal ground for doing this. However, the choice of legal ground affects the modalities of the processing and further processing. Moreover, with the GDPR's implementation, the available legal grounds have changed, and the European legalisation now provides a limited number of options.
- The **rights of the data subjects**: rights of the data subject, for example to be informed about the processing of their personal data, to obtain a copy, to have data erased under certain conditions, etc., are a key element as well. Under certain circumstances, some rights may be derogated. Additionally, these rights have been expanded and further defined by the GDPR, which also provides for exemptions specific to processing for scientific research. This is not, however, prescriptive and leaves room for interpretation.
- The implemented **safeguards**: safeguards, such as technical and organisational security measures, pseudonymisation, etc. are fundamental because they are the conditions with which researchers must comply when processing personal data, and, in particular, data concerning health. These safeguards are found in both national legislation and European legislation. As a result, they vary from one Member State to another.

This legal assessment will consecutively address: the rules applying to the processing of data concerning health in general, the regimes for processing such data for scientific research purposes under the Directive and the GDPR, and their respective national implementation.

[16] DoW, WP7, Annex1 (Part A) AEGLE Grant Agreement, p.33.

[17] Such as legislation applying to research or healthcare.

[18] See annex for the research protocol.



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. The rules applying to the processing of health data

In general personal data can be processed, but there must be a legal base or legal grounds justifying the processing.

Personal data can be organised in categories, such as basic identification data (name, address, patient's national identification number etc.), financial data (bank account number etc.). Some of these categories are legally qualified as "special", such as data revealing the racial origin, political opinions (affiliation to a political party etc.) or health data. **In principle, the processing of these special categories of data is prohibited.**[19] This principle was set out in the Directive and still applies under the GDPR. The prohibition of processing relies on the fact that, because of the nature of such data, its processing could infringe upon the fundamental freedoms or the privacy of data subjects.[20] This is why they require **a higher degree of protection**.

The 1995 Directive has set out the following list of special categories of data: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".[21] Under the GDPR, this list is now complemented by "genetic data, biometric data […] sexual orientation".[22] Moreover, unlike the Directive, the GDPR gives a definition of what is data concerning health: "'*data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*".[23] Defining the notion of health data in EU legislation avoids having a diverging interpretation of the notion at the Member State level, as might have been the case under the Directive. Similarly, the GDPR defines genetic data as well: "'*genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*".[24] While these categories might have been considered as special categories of data in some Member States under the Directive, their inclusion in the special categories of data ensures a harmonised, if not a uniform, regime across the EU.

Despite the general prohibition, the **processing of health data may sometimes be necessary**, which is why the Directive provided for **exceptions.**[25] In practice, they take the form of 'exemptions' and they are specific authorisation to process special categories of personal data. The first exemption to the principle was the **explicit consent** of the data subject. This prohibition also did not apply when the data was processed for the purposes of preventive medicine, **medical care** and diagnosis or the management of health services. However, this second exemption was subject to the processing only being carried out by a medical or healthcare processional or someone subject to an equivalent obligation of confidentiality. Additional **exemptions may have been laid down by the Member States** by two means, either by law or by a supervisory authority's decision. However, these exemptions had to be based on a substantial public interest.[26] These were the most relevant exceptions to the principle, to which could be added the situation in which the data was manifestly made public by the data subject him/herself.

[19] Article 8(1) DPD.

[20] Recital 33 DPD.

[21] Article 8(1) DPD.

[22] Article 9(1) GDPR.

[23] Article 4(15) GDPR.

[24] Article 4(13) GDPR.

[25] Article 8(2) DPD.

[26] Article 8(4) DPD.



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 Directive contained a list of exemptions and left the choice to the Member States to provide for additional exemptions to the principle.[27] The situation is now different under the GDPR. In the Regulation, the list of possible exemptions is exhaustive.[28] The exemptions existing under the Directive remain available under the GDPR, but the European legislator added other legal grounds legitimising the processing of health data. Since 25 May 2018, data concerning health, and other special categories of data may also be processed: for the establishment, exercise or defence of legal claims, for reasons of substantial public interest, on the basis of Union or Member State law,[29] for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, for archiving purposes in the public interest**, scientific or historical research purposes** or statistical purposes.[30] [31]

Moreover, while the exhaustive list of legal grounds for the processing of special categories of personal data in the Regulation allows **Member States to maintain or introduce further conditions and possible limitations to the processing of genetic data, biometric data and data concerning health,**[32] this permission would constitute a first 'backdoor' into the GDPR, which would enable the Member States to maintain or develop their own systems of health data, genetic data and biometric data processing. This provision does not give way to an additional legal base, it simply allows the Member States to set out further conditions or limitations upon the processing of such data. However, this action should not be a limitation upon the cross-border processing of such data. [33]

The approach adopted by the European legislator in 1995 was to prohibit the processing of health data and other special categories of data, and to provide exceptions to this principle. This was one way to address the special nature of such data; Switzerland provides an alternative way. While Switzerland is not a member of the European Union, it falls nonetheless within the scope of this legal assessment. The approach taken by the Swiss federal legislator has been different to the Union's legislator. Instead, while the processing is allowed, as for any other categories of data, it is subject to additional safeguards.

***Switzerland - see report p. 7***
*"Not being an EU Member State, Switzerland was and is under no obligation to implement Directive 95/46. While the creation of the DPA was influenced by Directive 95/46, the DPA does not prohibit the processing of health data. Nevertheless, the Swiss framework does provide for specific safeguards with regard to health data."*

Under EU legislation the principle is the following: data concerning health and other special categories of data cannot be processed. However, there are several exceptions to this principle, for example for providing health care or conducting scientific research.

[27] Article 8(4) DPD.

[28] Article 9(2) GDPR.

[29] This action is subject to specific conditions, and "shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject" Article 9(2)(g).

[30] This action is also subject to a specific condition, which will be addressed at a later stage of this report.

[31] Article 9(2)(f; g; h and j).

[32] Article 9(4).

[33] Recital 53; *in fine*, GDPR.



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. The processing of health data for scientific research purposes under Directive 1995/46/EU

Under the Directive, there was a general prohibition on the processing of data concerning health. However, provided adequate exemptions applied, processing was permitted. This section will explain: under what conditions health data could be processed under the Directive, what were the rights of the data subjects, and what were the expected safeguards.

## 3.1 The regime set out in the Directive:

None of the exceptions indicated by the Directive covered clearly or directly scientific research; however, they were the only possible legal bases. To determine which of the exemptions indicated in the Directive would have applied to scientific research, it must be kept in mind that scientific data may rely on both primary and secondary processing. In either case an adequate legal base is necessary.

- **Primary processing of health data for scientific research purposes**

In the case of the primary use of health data, the prohibition on processing may be overcome by a data subject's explicit consent.[34] The often overlooked issue is that this consent needs to be fully informed to be effective. This fundamental aspect of obtaining consent is left to ethics committees to police and monitor. Here, **explicit consent** must be understood to mean express consent, which means that consent is given "*by engaging in an affirmative action to express their desire to accept a form of data processing*".[35] Moreover, the Member States had the power to set additional exemptions to the general prohibition,[36] but as seen earlier, this was subject to a substantial public interest condition and the provision of suitable safeguards. It follows from Recital 34 of the Directive that scientific research was understood by the Directive as likely of being of public interest. :

> *"Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as […] scientific research […]; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals";*

'Public interest' here must be understood as what is not 'private interest'. A project of public interest must ultimately be of benefit to society, and not cater exclusively to the needs of its promoter.[37] But the means of regulating scientific research, when based on the processing of special categories of data, were left to the Member States. However, compliance of those legal provisions with European law was dependent on the Member States' provision of specific and suitable safeguards.

- **Further processing of health data for scientific research purposes**

Some scientific research in medical, biomedical, life and health sciences can require the re-use of personal data. This means that researchers use data that was initially collected for a different purpose, most often for the provision of health care. However, the secondary use of personal data is only accepted if it is not incompatible with the purpose

[34] Article 8(2)(a) DPD.

[35] Article 29 Working Party, WP187, Opinion 15/2011 on the definition of consent, p. 26.

[36] Article 8(4) DPD.

[37] Expertise juridique sur l'intérêt public dans le contexte des données de santé, Institut National des données de Santé, 29 Juin 2017, https://www.indsante.fr/sites/default/files/Documents_publics/rapport_dexpertise_juridique_sur_l_evaluation_de_linteret_public.pdf



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

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

of the data's primary use. In the case of scientific research, the Directive provided already for a presumption of compatibility with the initial purposes.[38] More specifically, scientific research purposes were not incompatible with the initial purpose if the Member States provided appropriate safeguards. This approach also meant that an additional legal base was not necessary; further processing is done on the legal base of the initial processing. This means that the legal ground justifying the collection of personal data for providing healthcare to the patient or subject for example the agreement between the healthcare provider and the patient, was sufficient for re-using the data afterwards for research purposes.

The processing of health data for scientific purposes was briefly regulated by the Directive. The principles of data quality applied, with an additional 'quality' necessary in the case of further processing together with a specific legal base, either based on the data subject's consent, or based on a legal ground established in national law. This last legal ground was subject to the provision of specific and appropriate safeguards. This basic regime left a wide range of manoeuvre for the Member States to regulate and organise the processing of personal data, in particular health data, for scientific research purposes.

- **The rights of data subjects**

The Directive ensured certain rights for the data subjects in certain circumstances, such as: the right to be informed of the processing, the right to access the data processed, and the right to object to the processing. The controller was under an obligation to inform data subjects; this obligation to inform data subjects about how their personal data was being processed was a corollary to the principle of fair processing. The information given had to be accurate and provided in a manner corresponding to the means of collection. There were two situations regarding data subjects' information. The first was when the personal data was collected directly for a data subject.[39] One example was a clinical trial. In this situation, the data subject had to be informed about the identity of the data controller or of its representative and of the purpose of the processing. The second situation envisaged by the Directive concerned the data subject's information when the data was not collected directly from him/her.[40] This scenario covered the situation of further processing and was also particularly relevant to scientific research, which often relies on pre-existing data sets. In this situation, the data controller had to inform data subjects when the data was collected, or at the latest when the data had been disclosed to a third party (i.e. researchers). The information to provide is the same as when the data was collected directly from the data subjects. However, the Directive indicated that this obligation did not apply when data was processed for scientific research purposes if the information would have been impossible to provide or that it would have required a disproportionate effort, of if the disclosure was expressly laid down in the law. But in these circumstances the Member States should have established appropriate safeguards.[41]

Under the Directive, data subjects had a right of access to the data.[42] Upon request, data subjects could obtain: confirmation of the processing, the purpose of the processing, categories of data concerned, recipients and categories of recipients, the communication in intelligible form of the processed data, and an explanation of the logic behind the automated processing. Moreover, data subjects could obtain the rectification, erasure or blocking of the processing of data when doing so did not comply with the principles set out in the Directive. Finally, the

[38] Article 6(1)(b) DPD.

[39] Article 10 DPD.

[40] Article 11 DPD.

[41] Article 11 DPD.

[42] Article 12 DPD.



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

controller must have notified such rectification, erasure or blocking, to data recipients unless it was impossible or required a disproportionate effort.

The Directive also provided the **right to object to the processing**. This right to object to the processing was strictly framed. The objection to the processing was only possible **when the processing was performed on the basis of the controller's legitimate interest, or when performed for the purpose of the task of public interest** unless specific national legislation applied. The objection must have been **based on compelling, legitimate grounds**. Neither of those two situations covered the processing of special categories of personal data for scientific research. It was left to the national legislator to decide whether there should be the right to object in another situation. **Establishing a right to object to the processing of personal data for scientific research purposes would pose a serious threat to scientific research based solely on the processing of data.**

- **Possible exceptions to the exercise of data subjects' rights**

The Directive also set out some **possible exemptions and restrictions on data subjects' rights**. Notably, there was a possible exemption of the obligation to inform data subjects when the personal data was not obtained directly from them, which was relevant in particular to the obligation to inform data subjects in the event of further processing. This exemption applied in the case of scientific research, if it was **impossible** or would have required a **disproportionate effort**; this exemption was subject to the implementation of **appropriate safeguards.**[43] Under the same conditions, the right of access may have been derogated as well.[44]

## 3.2 The implementation of the Directive in the Member States

The transposition of the Directive in the EU Member States did not ensure a uniform regime for the processing of health data for scientific research purposes. The legal grounds upon which the processing for scientific purposes was based varied, the safeguards were different, and the rights differed. The regime laid out in the Directive was only a starting point, and Member States stretched it during its transposition to fit scientific research.

### 3.2.1 Use of health data collected for research as a primary purpose

As seen earlier, the processing of special categories of data for scientific research was not specifically allowed by the Directive, but there was the power for the Member States to insert exemptions into data protection law or specific legislation (*lex specialis*) on scientific research. Together with the options provided by the Directive, there were **four main possible legal grounds**. The following figure (Figure 2) illustrates the proportion of each legal ground found during the analysis of the national country reports performed for this legal assessment:

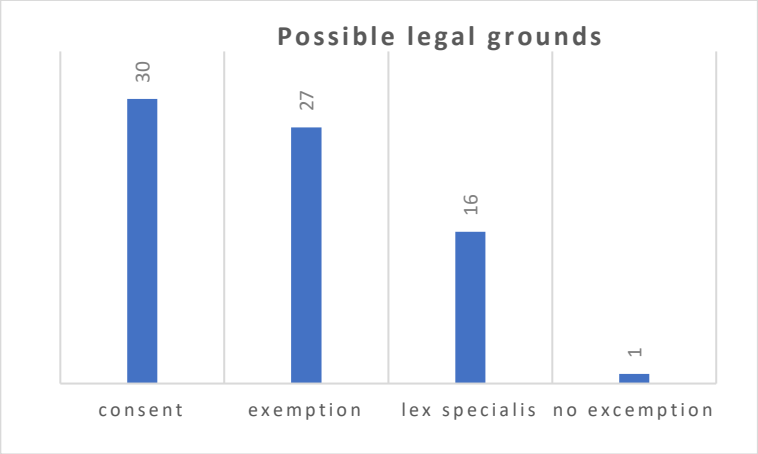
[43] Article 11 (2) DPD.

[44] Article 13(2).



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




| Possible legal grounds | Countries |
|---|---|
| Consent | All |
| Exemption | All but CY, LV and CH |
| *Lex specialis* | BG, CY, DK, FR, DE, EL, HU, LV, LT, NO, PT, RO, SK, SI, CH, NL |
| No exemption | HR |

**Figure 2: Possible legal grounds**

- **Consent**: consent was the first legal base for the processing of special categories of data laid out in the Directive.[45] As such, it is present in all legal frameworks. Such consent must have been explicit, as opposed to the simple, unambiguous consent required by Article 7(a) of the Directive. Usually, explicit or express consent is given in writing with a hand-written (or digital) signature, and more generally explicit consent must result in an affirmative action.[46]
- **Research Exception in Data Protection Acts**: As described above, the Directive gave the Member States the opportunity to lay down a research-specific exemption to the general prohibition for scientific research, through the application of Article 8.4.[47] For the purpose of this legal assessment, it is understood that research exemption means a research-specific exemption placed in the national Data Protection Act (i.e. Finland) or the provision of a *lex specialis*. A research exception can also take the form of a general authorisation by the supervisory authority (i.e. Italy).
- ***Lex specialis***: The Directive did not specify where the exemption must be inserted. It could be in specific legislation applying to scientific research, independent of the Data Protection Act (i.e. Latvia). This did not mean that a Data Protection Act did not apply. Often the *lex specialis* organised the applicable safeguards, and the Data Protection Act also contained the exception for scientific research (i.e. Portugal).
- **No exemption**: In this situation the Directive's national transposition did not provide for a research-specific exemption. In such a situation, the processing had to have happened on the basis of anonymised data or with the data subjects' consent (i.e. Croatia).

These possible legal grounds were not exclusive of each other. Consent was always an option. It was even the favoured option of most national legislation. A research-specific exemption and *lex specialis* often went hand-in-hand. Indeed, if the Data Protection Act gave the opportunity to process personal data for scientific research purposes, often the specific safeguards were indicated in the *lex specialis* (i.e. Portugal). The data protection law might have been the sole legal basis and indicated what the applicable safeguards were (i.e. Malta).

It is important to note that the *lex specialis* or the exemption for processing for scientific research purposes might have required the data subjects' consent. Processing without data subjects' consent of data identifying them (directly or indirectly)was possible in twenty-five (25) Member States.

[45] Article 8(2)(a).

[46] Article 29 Working Party, WP187, Opinion 15/2011 on the definition of consent, p.25.

[47] Article 8(4) DPD.



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

***Finland***[48]
*"Other derogations from the general prohibition for processing special categories of data are provided in Section 12 Sub-section 1 paragraph 6 of the Personal Data Act, under which it is permitted to process data for the purposes of historical, scientific or statistical research. Data subjects' rights are set out in Sections 24-29 of the Personal Data Act."*

***Italy***[49]
***"Authorisation no. 9/2014 - General Authorisation to Process Personal Data for Scientific Research Purposes,*** *concerning medical, biomedical or epidemiological* ***research.***
*The authorisation shall stipulate that the processing of health data for research purposes, can be carried out* ***even in the absence of consent****. The authorisation in fact concerns the processing of data subjects' data to be included in research, who cannot be contacted to provide information. The authorisation shall be issued to universities, other research bodies or institutes, and scientific societies, as well as to researchers and to those specifically appointed in charge of processing; such as managers, and therefore includes researchers."*

***Latvia***[50]
*"The legislator of Latvia did not insert any additional exemptions for the processing of health data for research purposes. The Law on the Rights of Patients states the following:*
*Patient records in* ***medical records may be used*** *in research if one of the following criteria is met:*
1) *the patient cannot be directly or indirectly identified on the basis of the information to be analysed;*
2) *the patient has agreed in writing that information about him/her is used in a particular piece of research."*

***Portugal***[51]
*"The special situations in which consent may be waived or dispensed must have a legal justification, e.g. the special situations foreseen under Article 19 § 6 of Law 12/2005 of 26 January […].*
*Law No 12/2005 allows that in cases of retrospective use of biological material and DNA samples in which the consent of the data subjects has not been collected, neither could it have been obtained due to the amount of data or death of any data subject, the ground of legitimacy for the lawful processing of personal data may derive from the provisions of Article 19 (6) of this law. "*

***Croatia***[52]
*The Croatian regulator did not make use of the power granted to Member States in Article 8.4 of the Directive by setting out additional exemptions."*

***Malta***[53]
*"[…] processing of sensitive personal data is permitted for research and statistical purposes provided it is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed. This is also subject to approval by the IDPC acting in accordance with its advisory body […]."*

[48] Cf. Doc. 11. Finnish legal framework, p.6.

[49] Cf. Doc. 17. Italian legal framework, p. 9.

[50] Cf. Doc. 18. Latvian legal framework, p.8

[51] Cf. Doc. 24. Portuguese legal framework, p.11.

[52] Cf. Doc. 06. Croatian legal framework, p. 8.

[53] Cf. Doc. 21. Maltese legal framework, p. 7.

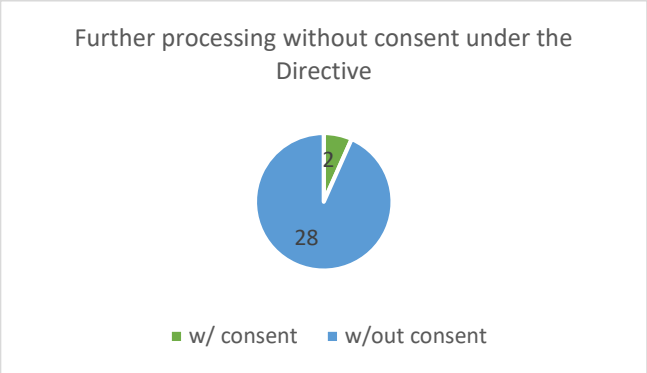


Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

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

### 3.2.2 Reuse of health data for research as a secondary purpose

Further processing is essentially the reuse of data collected for another purpose. In general, this reuse of data is allowed only if the **new purpose of processing is compatible with the initial purpose of processing**. However, in the case of scientific research, the compatibility of the purposes is **presumed.**[54] More accurately, the processing will not be considered to be incompatible, which is different. This is not intended to be understood as a blanket exemption to the compatibility requirement,[55] nor as a general authorisation to further process data for scientific research purposes. This **new processing must have the same legal base as the initial processing**, as seen above. The legal base, when dealing with scientific research can **either** be consent, **or** the possible exemption set out by national law, either in the Data Protection Act or in the *lex specialis*. Moreover, further processing for scientific purposes must be framed by **appropriate safeguards**. These safeguards are bound to differ from one Member State to another. The following figure (Figure 3) indicates the proportion of Member States in which **further processing without consent was admissible**:




| Further processing | Countries |
|---|---|
| With consent only | PL and HU |
| Without consent | All but PL and HU |

**Figure 3: Further processing without Consent under the Directive**

The specification of additional safeguards was left to the Member States' specific laws, which leaves rules for code of conduct (for example, the Netherlands, where pseudonymisation is required by Guidelines and not by legislation).

***The Netherlands[56] - see report p. 10***
*"The data should be pseudonymised before it leaves the treating physician. Yet, that does not follow from Dutch data protection law but from the clinical research guidelines, such as the GCP (Guidelines for good medical practice)."*

### 3.2.3 The data subjects' rights

As seen above, the Directive provided for data subjects' rights, and also for possible exemptions to those rights.

The transposition of those exemptions varied between the Member States, and not all legislation transposing the Directive provided exemptions on the controller's obligation. But the possible exemption to the obligation to inform was not left to the choice of the national legislator. Only Switzerland's legislation did not set out this power. By contrast, exemptions to the right of access and right to object to the processing were left to be determined by

[54] Article 6(1)(b).

[55] Article 29 Working Party, WP 203 Opinion 03/2013 on purpose limitation, p. 13.

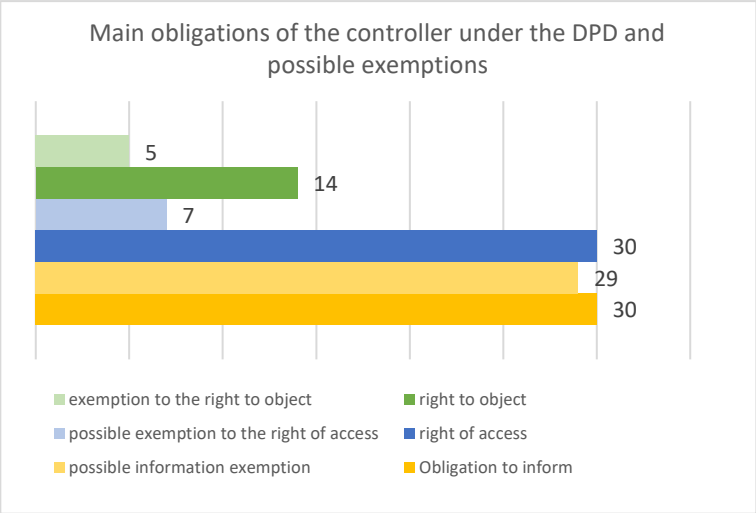
[56] Cf. Doc. 31. Dutch legal framework, p.12.



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

national law, and only a minority of legislators took up that opportunity. The graph below (Figure 4) represents the three main obligations of the data controller, relating to the rights of data subjects, and the possible exemptions implemented in national law across the thirty (30) countries evaluated for the purpose of this legal assessment.




| Rights and exemptions | Countries |
|---|---|
| Information | All |
| Information exception | All but CH |
| Right of access | All |
| Exemption of right to access | CZ, FI, FR, IT, LU, MT, NL |
| Right to object | BE, CY, DE, FR, DE, EL, HU, IE, LV, PT, RO, ES, CH, NL |
| Exemption to the right to object | BE, DK, FR, IE, RO |

**Figure 4: Main obligations of the controller under the DPD and possible exemptions**

The opportunity to object to the processing was granted in national law, and so was the opportunity to access the data. Only fourteen Member States gave a general right to data subjects to object to the processing of their personal data, such as Spain. Among those fourteen Member States, five provided for an exception to the right to object for scientific research, such as Ireland; only seven Member States provided an exemption to the obligation to grant access to data subjects, in the case of processing for scientific research purposes, such as Malta. A distinct lack of harmonisation could be observed concerning data subjects' rights. Even when the rights have matched, the safeguards set out as a condition for their exemption have varied.

***Spain***[57]
*"[…t]he data subjects will be able to claim their ARCO rights (the right to access, rectify, suppress and oppose the use of their data)."*

***Ireland***[58]
*"Section 6A transposes the right to object provided for in Article 14 of the Directive. Section 6A gives data subjects the right to request a data controller at any time to cease or not to begin the processing of personal data relating to them. The right to request a data controller to cease processing personal data can be used where the processing of the data causes or is likely to cause substantial damage or distress to the data subjects or to another person, and the damage or distress is or would be unwarranted. This right does not however apply in relation to the processing of personal data for medical research purposes."*

[57] Cf. Doc. 28. Spanish legal framework, p. 32.

[58] Cf. Doc. 16. Irish legal framework, p. 14.



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

### 3.2.4 The suitable safeguards

These safeguards must be provided for further processing as much as for scientific research in general. The Directive set out the adoption of suitable safeguards as a cumulative condition, related to a legal base, for the processing of special categories of data for research purposes,[59] and also for further processing in general.[60]

The **safeguards varied from one Member State to another**. In practice, this meant that the regime applying to scientific research varied from one Member State to another. Although the logic was the same, because it was set out by the Directive, different legal bases applied, as well as different categories of suitable safeguards. For projects involving the processing of data from different countries this meant the **cumulated compliance** with different sets of rules. The national country reports show a variety of possible safeguards; however, they can be organised into different categories as shown in Appendix A .

The **Directive indicated possible safeguards**, but they are not necessarily taken up by the national legislation or as guidelines set out by the national supervisory authorities. Additionally, the Commission regretted, in a report of 2003 on the Directive's implementation, the Member States lack of adoption of sufficient safeguards for further processing for historical, statistical or scientific purposes, as allowed by Article 6 (1)(b) of the Directive.[61]

The most frequent safeguards found in Europe have been the following:

- **Professional secrecy**[62] was a possible safeguard suggested by the Directive or processing under the supervision of a health professional.[63] The obligation to ensure the personal handling of the data was subject to professional secrecy, as a result of a statutory or contractual obligation. This is also linked to the requirement of processing confidentiality.[64]

- **Encryption**: the terminology used varied, (i.e. coded or anonymised). Oftentimes National legislation indicates data processed for scientific research purposes should be fully anonymised, which would take it outside the scope of legislation applying to personal data. However, very often relying exclusively on anonymised data is not possible when data is processed for scientific research purposes. This is why, to protect as much as possible data subjects' privacy, national legislation introduced a gradation in the encryption of the data. When research requires distinguishing individuals, it indicates that data processed can be coded, or pseudonymised, if necessary for research purposes. But, sometimes this step might not be sufficient and identifying data might be required. In such circumstances, the reasons for such processing must be demonstrated to the supervisory authority, or another competent body. This is the case for example in Belgium, or in Portugal.

- **A processing authorisation by the supervisory authority** is very often required. However, here too there were different situations.

    - Specific, cluster, or general: the form of the authorisation varied from one Member State to the other, but also due to the specificities of research projects. Often, the processing authorisation concerned a research project (i.e. France). But sometimes (i.e. in Denmark) the authorisation was

[59] Recital 34 DPD.

[60] Recital 29 DPD.

[61] European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, p. 18.

[62] Recital 33 DPD

[63] Recital 42 DPD.

[64] Article 16 DPD.



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

an 'umbrella' authorisation, where an institution asked for authorisation for a research project on an annual basis. In other cases, there was a sectorial authorisation or a general authorisation, such as in Italy, where the Guarantee[65] adopted a general authorisation for biomedical research, provided that the project meets certain criteria.

- Identifying or indirectly identifying data: in some Member States, the requirement for the authorisation of the supervisory authority depended on the degree of encryption (or lack of it) of the processed data (i.e. Estonia).
- For further processing only: in other Member States, the authorisation of the supervisory authority was only required for further processing (i.e. Luxembourg).

- **Approval or vetting by an ethics committee**: approval by an ethics committee can be linked to the requirement of an ethical vetting set out by the Regulation on clinical trials. Despite the fact that this requirement at the European level in Regulation 536/2014 on clinical trials on medicinal products for human use, applies to '*interventional studies*', and '*non-interventional studies*'[66] are outside of the scope of this regulation, thus placing research project based exclusively of further processing is a 'grey' area. Ethical approval or review of a project might be required nonetheless; in some countries, the ethical approval process has been integrated in more general procedures. For example, in France ethical approval is part of the procedure prior to the processing of health data. The results of the ethical evaluation are to be annexed to the notification of processing to the CNIL. A similar situation is found in Norway and Sweden.
- **Technical and organisational measures**: The processing of data had to follow relevant protocols, and adequate security measures must be implemented by the controller (i.e. reference methodologies in France).

***Portugal***[67]
*"In case the study cannot be carried out with irreversibly anonymised data, the use of coded data should be preferred, even if it can be converted to personal data by means of a decoding key. Access to this key must necessarily be limited to the main investigator, who is bound by professional secrecy."*

***France***[68]
*"The second category includes research studies or evaluations not involving human subjects. This is health research that does not belong to research involving human subjects. In particular, it is research requiring only the re-use of covered personal health data (e. g. from medical records, existing cohorts, or the National System of Health Data). For this category of research, CNIL's authorisation is necessary too. But the Controller will have to obtain CEREES' opinion (the expert committee for research, studies and evaluations in the field of health) prior to applying CNIL for its authorisation. CNIL has yet to adopt methodologies of reference for research not involving human subjects."*

***Denmark***[69]
*"In 2015, the Data Protection Agency made an organisational change of the notification system, so that it is not the individual researcher/research group, but the public authority, where the research is taking place (e.g. the university, or the Regional Council (for hospital research)), which must make a so-called "umbrella notification" covering all current and upcoming research projects. This means that the Data Protection Agency's role for research projects carried out in the public sector is rather limited, apart from approving the "umbrella notifications". For research projects carried out in the*

[65] The Garante is the Italian Data Protection Authority

[66] Regulation 536/2014 on clinical trials on medicinal, Articles 1 and 2

[67] Cf. Doc. 24. Portuguese legal framework, p. 13

[68] Cf. Doc. 12. French legal framework, p. 9.

[69] Cf. Doc. 09. Danish legal framework, p. 12



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

*private sector (e.g. industry-based research or research projects carried out by patient organisations or NGOs) the processing of data for research purposes must be notified to the Data Protection Agency, and the authorisation from the agency must be in place before the processing of data for research purposes can be initiated (Article 50 of the Act)."*

***Estonia***[70]
*"Based on the NDPA, if the scientific research is based on special categories of data (i.e. health data), the Ethics committee of specific field (or EDPI if there is no such Ethics committee) must check the compliance of the planned processing with the requirements under the law. This procedure does not apply if the data has been pseudonymised or anonymised."*

***Norway***[71]
*"Medical research concerning identifiable individuals in general requires both prior approval of the research as well as exemption from the duty of confidentiality of the health personnel involved in the project. The Health Research Act made the process for application for approval of medical health research more efficient due to the main principle in the Act that such an application only needs to be directed to one body, namely to the REK in the applicant's geographical area. There is, thus, no need to also seek a licence from the Data Protection Authority, or to apply for exemption from the duty of confidentiality from the Directorate of Health. This is because, upon the entry into force of the Health Research Act, the REKs took over the tasks that previously lay with the Data Protection Authority (i.e. licensing for the processing of health data) and the Directorate of Health (i.e. regarding the exemption from the duty of confidentiality and the approval of the setting up of research biobanks)."*

***SWEDEN***[72]
*"All research referred to in the Ethical Review Act may only be conducted where approval has been granted following an ethical vetting (Section 6 Ethical Review Act). Research involving the processing of personal data is only allowed where approval for this processing has been given as part of the ethical vetting."*

***FRANCE***[73]
*"The research may proceed once CNIL have given its authorisation. However, the CPP's (Person's Protection Committee) Opinion must be obtained prior to applying to the CNIL for its authorisation.*
*But CNIL's authorisation is not necessary if the research follows the referential methodologies detailed by CNIL, and that the controller has declared on CNIL's website that the research would be lead in conformity with that methodology.[1] This step considerably simplifies the procedure."*

Under the Directive, the option to process identifying health data for scientific research purposes (without data subject's consent) was organised by national legislation. In practice this lead to differentiated regimes between Member States. Data subjects' rights were different, and so were the safeguards in place. The situation was further complicated by disparities between the rules applying to the initial processing and rules applying to reuse of data.

[70] Cf. Doc. 10 Estonian legal framework, .p. 6.

[71] Cf. Doc. 22. Norwegian legal framework, p. 12.

[72] Cf. Doc. 29. Swedish legal framework, p. 10.

[73] Cf. Doc. 12. French legal framework, p. 9



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

# 4. The processing of health data for scientific research purposes under the GDPR

The GDPR has applied since 25 May 2018. As a Regulation it is directly applicable in the Member States and does not require any transposition measures. However, the GDPR provides about fifty open clauses that give the Member States further opportunity to regulate. This is why all new national legislation concerning the GDPR must accordingly modify national rules. Some of the cases where the GDPR leaves some leeway to the Member States apply directly to scientific research.

## 4.1 The regime set by the GDPR

The main principles set out in the Directive remain valid under the GDPR. However, the logic of the legislative changes and the **principle of accountability** have become prominent. It is now the controller's responsibility to demonstrate how its activities comply with the applicable rules. This section will nonetheless consecutively address: the legal grounds, the data subjects' rights, and the applicable safeguards when processing special categories of data for scientific research purposes.

### 4.1.1 Use of health data collected for research as a primary purpose

The use of data concerning health and genetic data for scientific research can be justified by two of the legal grounds set out in Article 9 of the GDPR, either: consent,[74] or processing for scientific research purposes.[75]

In the case of processing for scientific research purposes, some of the requirements set out by the Directive in Article 8.4 can be found as well, such as suitable safeguards. However, Article 9(2)(j) sets **new conditions**. The first condition is **necessity**. The processing of personal data is permitted, if it is the only means available to achieve the aim of the research project. Secondly, the processing must comply with the **safeguards** set out by the GDPR concerning processing for scientific research purposes.[76] Thirdly, this legal ground is not sufficient of itself, it must be **supplemented by another Union or Member State legal ground,** and finally the processing must be **proportionate** to the aim being pursued, **respecting the essence of the right of data protection** and providing suitable and specific measures for safeguarding data subjects' fundamental rights and freedoms.

Article 89(1) GDPR sets safeguards and derogations relating to the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. **Article 89(1) is key to the regime for scientific research set out in the GDPR**. The foreseen potential exemptions only apply if there is adherence to the principles set out in Article 89(1). This provision should be read in parallel with **the principles of privacy by design and by default.**[77] Indeed, the measures required by the Article 89(1) should be envisaged at the start of the research project and included in the research protocol early on. This way they are less likely to disrupt the research 'flow'.

The safeguards set out by this Article will be addressed later, but already the GDPR indicates that technical and organisational measures as well as pseudonymisation should be used by the controller. Moreover, **the Regulation favours "further processing which does not or no longer permit the identification of data subjects"** and seems to imply it is already a kind of safeguard for the rights and freedoms of data subjects.

[74] Article 9(2)(a) GDPR.

[75] Article 9(2)(j) GDPR.

[76] Article 89(1) GDPR.

[77] Article 25 GDPR.



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

### 4.1.2 Reuse of health data for research as a secondary purpose

As under the Directive, further processing is envisaged in the GDPR. However, a number of conditions must be met. Primarily the processing must not be incompatible with the initial purpose of processing. The GDPR, as the Directive did before it, sets out a **presumption of compatibility** in favour of scientific research. Article 5(1)(b) states:

> *"[…] further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');"*

However, to ensure this presumption of compatibility, the processing must comply with Article 89(1) of the GDPR, set out above. This means **the appropriate safeguards must be in place**. In the case of further processing, the legal base does not need to be different from the *legal base* used for the initial processing.[78] Consent would be acceptable, if data subjects have been informed of the further reprocessing upon the collection of data. If the processing was initially based on Article 9(2)(j), further processing must be based on this Article as well. However, the GDPR makes the processing of personal data for scientific purposes conditional upon additional legal grounds, which can be found either in Union law or in Member State legislation.[79] In this instance, the GDPR fosters a lack of coherence in the regime applied to scientific research.

### 4.1.3 The rights of data subjects

The rights of the data subjects have been developed under the GDPR compared to the Directive. The obligation to inform has been strengthened significantly. However, when considering the regime applying to scientific research, the GDPR opens the door to a **differentiated regime** across Europe.

#### Informing data subjects

As under the Directive, **researchers have the obligation to inform data subjects**[80] of the identity and the contact details of the controller and, where applicable, of: the controller's representative, the contact details of the data protection officer, and, where applicable, the purposes of the processing for which the personal data is intended as well as the legal base for the processing. Data subjects must be informed of the recipients or categories of recipients of the personal data, if any, and, where applicable, the fact that the controller intends to transfer their personal data. This information should be provided at the latest **when the data is collected**.[81] When the data is not collected from the data subjects (i.e. in the situation of further processing), then the data subjects should be informed within one month after the data have been transferred to the new controller.[82]

Article 14(5)(b) GDPR sets out a specific **exemption for scientific research**, on the condition that the processing performed complies with the principles set in Article 89(1) GDPR. According to this exception, the data subjects would not have to be informed if it were **impossible** or if it would involve a **disproportionate effort**. Additionally, this exemption applies also where the consequences of the obligation to inform are likely to make impossible or seriously impair the achievement of the objectives of the processing for scientific research purposes. In such circumstances the controller must take other measures to ensure the protection of the data subjects' rights and

[78] Recital 50 GDPR.

[79] Article 9(2)(j) GDPR.

[80] Articles 13 & 14 GDPR.

[81] Article 13 GDPR.

[82] Article 14 GDPR.



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

freedoms. This is particularly pertinent when there is a mandate to make the information from the data available under open access.

Although the GDPR sets out possible exemptions for the obligation to inform the data subjects, they are specific, and **may not be routinely relied upon by researchers.** This would be contrary to the principle under which processing for scientific research must comply with safeguards for the data subjects' rights and freedoms. The impossibility to inform data subjects must be absolute. This means it must **there must be no possible means of** informing data subjects. If the controller seeks to apply this exemption, then he/she must be able to demonstrate the factors actually preventing the provision of information.[83] The criteria of the 'disproportionate effort' cannot be casually used either to be exempted from the obligation to inform the data subjects. Moreover, the 'impossibility to inform' or the 'disproportionate effort' it involves must be a consequence of the fact that data was obtained from sources other than the data subjects. The effort required to inform the data subjects should be evaluated on the basis of a **balancing exercise**, that should be documented by the controller. In the case of pseudonymised data, the controller should not be required to obtain new data to be able to inform the data subjects that their data is being processed.[84] Finally, the controller may be exempted from the obligation to provide information to data subjects if it **would seriously impair the objectives of the research project**. In this scenario, the information would have to nullify the objectives of the processing.[85]

- **Right of access**

Data subjects have the right to obtain from the controller the **confirmation** that their personal data is being processed. They have the right to access the processed data[86] and obtain information on: **the purpose of the processing, the categories of data concerned**, the categories of recipient to whom data will be or is being disclosed, the envisaged storage period, or the criteria used to set that period, the existence of the right to request rectification or erasure of personal data or the restriction of the processing or the right to object to the processing or the right to lodge a complaint to the supervisory authority. If data is not collected from the data subjects, then the information provided should include the source of the data.

- **Right of rectification**

Data subjects may request and obtain from the controller the **rectification**[87] **of inaccurate data**. In certain circumstances, data subjects have the right to obtain from the controller the erasure of the data concerning them.[88] However, there is a specific exemption applying to scientific research.[89] The GDPR provides directly for this exception, whereas the others must find an additional legal ground in Member State law (see below). When data subjects exercise their rights, notably to correction, or erasure data concerning them, or simply object to the processing, then the controller must restrict the processing activities applied to the data concerned.[90] This situation also applies when the data is **no longer needed** but is simply stored because it is required by data subjects for the establishment, exercise or defence of legal claims. In such a situation, data subjects must give their consent to any

[83] WP 260, Article 29 working party's Guidelines on transparency under Regulation 2016/679, §52, p. 26.

[84] WP 260, Article 29 working party's Guidelines on transparency under Regulation 2016/679, §§ 54-57, pp. 27-28.

[85] WP 260, Article 29 working party's Guidelines on transparency under Regulation 2016/679, § 58, p. 28.

[86] Article 15 GDPR.

[87] Article 16 GDPR.

[88] Article 17 GDPR.

[89] Article 17(3)(d) GDPR.

[90] Article 18 GDPR.



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. When the restriction is lifted, the data subjects must be informed. In certain circumstances, which is when the data is processed based on consent or following a contract, and the processing is carried out by automated means, then data subjects have the right to receive the personal data concerning them that they have provided.[91] This right applies to data concerning the data subjects, not the profiles and analysis that have been made of the data, following the processing activity. This right may prove to be challenging for big data analytics, when data from various sources is processed by automated means.

- **Right to object**

Data subjects have the right to object[92] to the processing of their personal data at any time on grounds relating to their particular situation. However, **this right is limited. In the case of scientific research**, there is a specific exception[93] if the processing complies with the conditions set Article 89 (1) of the GDPR, unless the processing is carried out for a task of public interest.

- **Possible exceptions to data subjects' rights**

Article 89(2) GDPR indicates the opportunity for the Member States to provide **derogations to the rights** addressed above. This provision is not directly applicable to the data subjects but rather targets the Member States. It is an invitation for a more liberal regime for scientific research. But, at the same time, it creates a justification for a **reduced harmonisation of the European scientific research regi**me. However, there are conditions. Member States must ensure **appropriate safeguards.**[94] Moreover, this derogation only applies **in certain circumstances**. The right would have to be "*likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*".[95]

The Article 29 Working Party interpreted the conditions in the *Guidelines on transparency* addressed earlier. Effectively, the exercise of those rights would have to nullify the objective of the research for the derogation to apply.[96] The burden of proof regarding the serious impairment of the processing objective lies with the researcher.

### 4.1.4 The appropriate safeguards

The suitable safeguards are the **cornerstone** of the regime when applied to scientific research. If they are not implemented, then the regime does not apply. The safeguards are indicated in Article 89 (1) of the GDPR. While this Article provides some examples of what appropriate safeguards can be, this is **not an exhaustive list**. The safeguards must comply with the Regulation. Some of the controller's obligations concern scientific research.

The Regulation relies heavily on the **concept of accountability of the controller**. This means that the controller must be able to **demonstrate his/her compliance**. This requires being able to produce justification for the decision taken, and the adequate policies guiding such a decision.

- **Data Processing Impact Assessment**

[91] Article 20 GDPR.

[92] Article 21 GDPR.

[93] Article 21 (6) GDPR.

[94] Article 89(1) GDPR.

[95] Article 89(2) GDPR.

[96] WP 260 rev.01, Article 29 working party's Guidelines on transparency under Regulation 2016/679, §65, p. 31.



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

First, a Data Processing Impact Assessment[97] (DPIA) must be performed when the processing is **likely to result in a high risk** to data subjects' rights and freedoms. In particular, when the **processing concerns special categories of data at a large scale then a DPIA is required.**[98] There is a **dual condition**. The processing must be likely to result in a high risk for the rights and freedoms of natural persons and be the processing on a large scale of special categories of data. Large scale processing is not explicitly defined in the Regulation; however, the Article 29 Working party has advised paying particular attention to the number of data subjects, either by absolute value, or in proportion to the considered population, the volume of data processed, the duration of the processing and the geographical scope of the processing activity. Among these elements, the volume is relevant in the case of Big Data analytics, and the geographical scope of the processing, for a multinational research project. DPIA are also required when special categories of data are processed; one example, particularly relevant for scientific research, is the medical files kept by hospitals in which access to the information they contain may be requested for medical research purposes only. It is also recommended that a DPIA be conducted when processing is the "*storage for archiving purpose of pseudonymised personal data concerning vulnerable data subjects of research projects or clinical trials*".[99] Moreover, when it is not clear whether a DPIA is necessary, it is advisable to one should be carried out nonetheless, as it is generally useful to comply with data protection law.[100]

Conducting a DPIA will indicate the points to which particular attention must be paid security-wise and can point towards the adequate safeguards that could be implemented to limit the risks discovered. But a DPIA must not be the sole instance prompting reflection on the adequate safety measures to be implemented. Researchers must abide by the principles of security by design and security by default.[101] This means that adequate safeguards must be thoroughly considered at the inception of the project. This is something with which all scientific researchers are well acquainted. **Record of processing activities**

The GDPR requires researchers to maintain a **record of their processing activity**.[102] This record is an instrument for **demonstrating compliance** with the GDPR. It should contain: the name of the controller, the purpose of the processing, a description of the categories of data subjects and of personal data, a description of the categories of recipients, information concerning data transfers (if relevant), and, if possible, the envisaged time-limit for erasure, as well as a general description of the technical and organisational security measures implemented.

### Technical and organisational security measures

The security measures implemented must be devised whilst bearing in mind the context for and the purpose of the processing.[103] The measures include, as appropriate: the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[104] The measures taken should be **proportionate**

[97] Article 35 GDPR.

[98] Article 35(3)(b) GDPR.

[99] WP 248 rev.01, Article 29 working party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 04 October 2017, p 11.

[100] WP 248 rev.01, *op.cit.*, p.8.

[101] Article 25 GDPR.

[102] Article 30 GDPR.

[103] Article 32 GDPR.

[104] Article 32 (1) GDPR.



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 the cost** and the **technical and technological situation**. For a long-term research project, **periodical evaluation** and update of those measures would be necessary.

### Data Protection Officer

The appointment of a Data Protection Officer[105] (DPO) is also a safeguard provided by the Regulation. The controller, and the processor, if relevant, must appoint a DPO when **the core activity consists of the processing of large scale special categories of data**. The core activities are the controller's key operation, but they are not exclusive of activities in which the processing of data forms an inextricable part of the controller's activity.[106] For example, in scientific research, the core activity is to do research, and the processing of personal data is necessary for the performance of that activity. The criteria are otherwise the same as for the DPIA, i.e. the large-scale processing of special categories of personal data.

### Particularities for scientific research

While the general safeguards provided by the Regulation apply, Article 89 (1) emphasises some, in particular, technical and organisational measures in place that should in particular ensure data minimisation.

**Data minimisation** is one of the principles of quality of data,[107] but it is emphasised for scientific research. This implies a solid research protocol in which the purpose of the processing is clearly defined, so that **only the absolutely necessary data is used for the research**. This is especially challenging for Big Data, which relies on a certain volume of data the uses of which cannot be fully predicted at the inception of the project or construction of the database. It is also difficult for Big Data because the nature of future research projects cannot be predicted. Hence it is justified to have a wide dataset if the data is expected to have some value. The notion of data minimisation, and the preparation this requires should normally be done at the same time as the preparation of a scientific study.

**Pseudonymisation and encryption** are the first security measures suggested by Article 32 GDPR and are also suggested in Article 89(1) GDPR. Whilst this is not an obligation, it should, however, be the preferred method if possible (when anonymisation is not an option). Pseudonymised data are defined in Article 4 GDPR as data that can no longer be attributed to a specific individual without the use of additional information. There is an assumption that the risk to the rights and freedoms of the data subjects are reduced if the data is processed while pseudonymised. A basic pseudonymisation technique recommended by the GDPR is to keep the identifying data distinct form the rest.[108] This is a requirement in some Member States, and it is the type of measure that should be included in the research protocol.

**Further processing should also be privileged when possible**. Further processing is proposed as a safeguard in itself by the GDPR i.e. no "new" personal data is collected. In a sense, it is also in line with the principle of data minimisation. However, the data re-used for the further processing should not permit the direct identification of the data subjects.

Some Member States have adopted some additional safeguards, such as the requirement that processing in some cases still be notified, or that it must follow pre-established methodologies and/or protocols, or, as in some

[105] Article 37 GDPR.

[106] Article 29 Working Party, WP 243 rev. 01, Guidelines on Data Protection Officers, p. 7.

[107] Article 5(1)(c) GDPR.

[108] Recital 29 GDPR.



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

countries, that a specific pseudonymisation protocol is imposed. These safeguards are provided by Member States legislations that pertinent specifically to scientific research.

## 4.2 The implementation of the GDPR in the Member States

While the GDPR is directly applicable, its text leaves a number of options for the Member States to legislate further. Generally, across Europe the application of the GDPR has triggered a revision of the existing Data Protection Acts; these New Data Protection Acts (NDPA) provide further legislation which the GDPR has provided to the Member States.

There are two main 'backdoors' in the GDPR. The first is in Article 9(2)(j), which is the exception for the processing of special categories of data for scientific research purposes and requires that there be an additional legal base either in national law or in Union law. **This alternative route provides the opportunity for adding numerous requirements to scientific research based on the processing of personal data in different Member States**. The second alternative route is the opportunity available in Article 89(2) of the GDPR for a Member State to provide a derogation to some data subjects' rights. However, these derogations are subject to respecting **specific safeguards**. In addition to these two main 'backdoors' to the regime when applied to scientific research, there are other options left by the GDPR to the Member States that are relevant to scientific research in the medical, biomedical, life and health sciences. .

Article 9(4) GDPR indicates that some categories of the special categories of data, such as genetic data, biometric data, and data concerning health, are 'even more special'. Member States may introduce further limitations or conditions on the processing. (i.e. Belgium, as indicated in Article 9 of NDPA[109] )

The approach followed for the implementation of the open clauses of the GDPR varies from one Member State to another. Some have decided to amend the existing Act, while others have adopted a completely new Act and repealed the previous one. Beyond such modalities, the substance varies too. Some Member States have taken a minimalistic approach and kept as close as possible to the GDPR by implementing no or only a few 'backdoors', while others have made the most of the opportunities given to them.

### 4.2.1 Legal grounds of processing for scientific research purposes

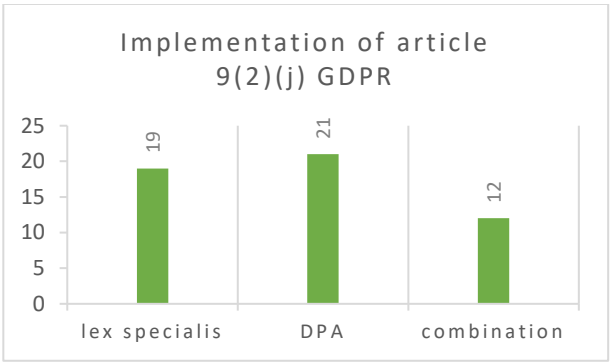
Consent remains under the GDPR the first possible legal ground for the processing of data concerning health. However, in the case of processing for scientific research purposes, Article 9(2)(j) is an alternative legal ground, enabling scientific research without data subjects' consent. However, **this GDPR provision cannot stand alone; it must be implemented**. There are several options for Member States, either through: a provision of the NDPA, or through *lex specialis*, or combination of both, and which is illustrated by the following figure (Figure 6):

[109] Although the Bill was adopted by the House of representatives, it still has to be formally enacted (26/07/2018)



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



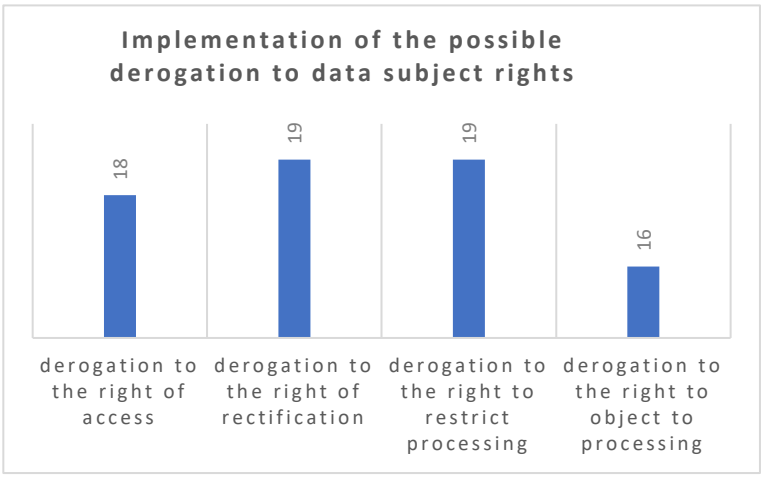

| Means of implementation | Countries |
|---|---|
| Lex specialis | AT, BG, DK, FI, FR, DE, EL, HU, IT, LV, LT, NO, PT, RO, SK, SI, SE, CH, NL |
| DPA | AT, BE, CY, CZ, DK, ES, FR, DE, IE, IT, LV, LU, NO, PL, PT, SK, SI, ES, SE, SE, NL, UK |
| Combination of the two | AT, DK, FR, DE, IT, LV, NO, PT, SK, SI, SE, NL |

**Figure 6: Implementation of Article 9(2)(j) of the GDPR**

From the data collected when preparing this legal assessment, we have observed that not all the Member States have decided to implement Article 9(2)(j) GDPR (for example, Croatia did not). However, in almost two-thirds of the Member States, existing *lex specialis* will continue to apply; so even though the NDPA does not specifically provide for scientific research, or if the Article 9 (2)(j) is not specifically implemented in the Act, the exception provided by the GDPR may still apply (i.e. Lithuania). However, the majority of the Member States have provided in the NDPA an exception for scientific research purposes (i.e. the UK).

### 4.2.2 The data subjects' rights

Some of the data subjects' rights addressed above may be derogated under certain circumstances. These possible derogations, as set out in Article 89(2) GDPR, are one of the 'backdoors' provided for data usage when applied to the scientific research. However, these **derogations are only possible when provided by Member State law**, and to the extent that the exercise of the right to access, rectification, erasure, or the right to object are likely to render impossible, or seriously impair the achievement of the scientific research purpose. The following figure (Figure 7) illustrates the implementation of the possible exemptions:




| HEADING 1 | HEADING 2 |
|---|---|
| Derogation to the right of access | AT, BG, DK, EE, FI, FR, DE, EL, IE, LU, MT, NO, PT, RO, EL, SE, SE, NL, UK |
| Derogation to the right of rectification | AT, BE, DK, EE, FI, FR, DE, EL, IE, LV, LU, MT; NO, PT, RO, ES, SE, NL UK |
| Derogation to the right to restrict processing | AT, BE, DK, EE, FI, FR, DE, EL, IE, LV, LU, MT, NO, PT, RO, ES, SE, NL, UK |
| Derogation to the right to object to processing | AT, BE, ES, FI, FR, DE, EL, IE, LV, LU, MT, , PT, RO, SK, SE, UK |

**Figure 7: Implementation of the possible derogations to data subjects' rights (This graph does not include, Hungary, Italy, and Switzerland)**



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

***Croatia***[110]
*"The Act Proposal does not further regulate the processing of health data for research purposes in any manner, nor does it implement Article 9 (2) (j). Therefore, the provisions of the GDPR shall be applied directly.*

***Lithuania***[111]
*"While the general data protection regime will be based on the GDPR, meaning that specific local provisions on notifications, prior-checking, safeguards related to scientific research, etc., will no longer apply, the specific regime applying to biomedical research will not be substantially affected by the GDPR. Therefore, conditions set out in the Patients' Rights Law and especially the conditions set out in the Biomedical Research Law will apply despite the GDPR, requiring researchers to complete the required steps and comply with obligations such as the aforementioned requirement to receive an authorisation from the Lithuanian Bioethics Committee or a regional biomedical research ethics committee."*

***United Kingdom***[112]
*"10. Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—*
*[…]*
*(c) point (h) (health and social care);*
*(d) point (i) (public health);*
*(e) point (j) (archiving, research and statistics).*
*(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorization by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1."*

**Not all Member States have taken the opportunity to provide for derogations** to certain rights of the data subjects (i.e. Slovenia). But some Member States have provided for the restriction on all the rights, such as Austria. Although this may in fact be an over-implementation because the exception of the right of erasure is already an option in the GDPR. Some Member States have given derogations with additional conditions to certain rights (i.e. Sweden). **Researchers collecting data from different countries will have to pay particular attention to such derogations**.

***Slovenia***[113]
*"Article 89 (2) GDPR provides the opportunity for derogations to: the right to access the data by the data subject, the right to rectify, the right to restrict the processing and the right to object. However, these derogations are only available if these rights seriously impair or make impossible the scientific purpose of the processing.*
*Since in the Act Proposal there is no such derogation, it appears that the government did not intend to build upon the opportunity to provide derogations to some rights of data subjects."*

***Austria***[114]
*"The following data subject rights do not apply under section 5 (7) FOG if the purpose under Article 89 GDPR is likely to be made impossible or seriously impaired: the right to access by the data subject (Article 15 GDPR); the right to rectification (Article 16 GDPR); the right to erasure (Article 17 GDPR); the right to restriction of processing (Article 18 GDPR); the right to data portability (Article 20 GDPR); as well as the right to object (Article 21 GDPR)."*

[110] Cf. Doc. 06. Croatian legal framework, p. 14

[111] Cf. Doc. 07. Lithuania, legal framework, p. 16.

[112] Cf. Doc. 18. British legal framework, p. 18.

[113] Cf. Doc. 27. Slovenian legal framework

[114] Cf. Doc. 03. Austrian legal framework, p. 15.



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

***Sweden***[115]
*"The Research Data Inquiry Committee also proposes that individuals should be able to challenge their personal data being processed for research purposes. If this option proves to be impossible or involves disproportionate effort, or if the purposes of the research cannot otherwise be attained, then the data may nevertheless be processed (Section 9 of the new Act)."*

### 4.2.3 The safeguards

As stated earlier, the GDPR's safeguards may be complemented by national legislation. The Member States may legislate in this domain and add additional safeguards for the data subjects or requirements for the controllers (Article 9(4), Article 36 (5), Article 23).

The most frequent safeguards under the Directive were the requirements concerning: professional secrecy, encryption, the authorisation from the data protection authority, or other competent authority, ethical approval by competent ethics authorities, and the technical and organisational measures. **Under the GDPR, some of the more frequent safeguards are already implemented at the European level**, while others have been made obsolete due to the change of rationale of the data protection legislation. The rationale has shifted from a prior control (based on the declaration of processing activities required by the Directive),to a control from the authorities after the beginning of the processing activities.

In most of the countries observed, the legislation directly governing scientific research has not yet been amended to reflect the change caused by the GDPR. A necessary transition period will see the cohabitation of the GDPR with general requirements and national legislation with requirements tailored for scientific research. Some Member States have made some changes to such rules when preparing for the GDPR's implementation (i.e. France and the Netherlands)

Often the Member States will organise the **modalities of the pseudonymisation**. (i.e. Belgium) and set out specific requirements, especially for the use of data from public data sets (i.e. data owned by hospitals or research institutions). The **conditions for ethics approval**, which are indirectly implied by the GDPR (with its reference to clinical trial regulation), vary from one Member State to another. The processing of genetic data is often further regulated (possibly under Article 9.4) i.e. Denmark; Italy. Some Member States seek to strengthen the GDPR requirement by including them as safeguards in their national law, (i.e. Luxembourg; Ireland). Consultation or **notification to the supervisory authority may be a retained safeguard** (i.e. Greece, Austria or France).

***Germany***[116]
*"According to the section [ section 27], the controller shall take appropriate and specific measures to safeguard the interests of the data subject. A reference to section 22 (2), second sentence is made which makes clear that for evaluating which measures are appropriate, the controller should take into account: the 'state of the art', the cost of implementation and the nature, scope, context and purposes of processing as well as the risks for the data subject posed by the processing. Section 22 (2) also states specific safeguards that controllers may use. Section 27 (3) of the new FDPA requires that additionally the personal data shall be made anonymous as soon as the research or statistical purpose allows, unless this conflicts with the*

[115] CF. Doc. 29. Swedish legal framework, p. 19.

[116] Cf. Doc. 13. German legal framework, p. 25.



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

*legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately."*

***Italy[117]***

*"The unofficial proposal of the Legislative Decree, to implement the GDPR, should not have too many consequences for the national legal framework regarding data re-use for scientific research or statistical purposes. The Italian legislator seems to have introduced a stricter requirement since it allows for the Garante to give an Authorisation to re-use data, even for the processing of special categories of data as laid down in Art. 9(2(j)) GDPR, but places a clear barrier of exclusion for such re-use of genetic data."*

***Ireland[118] - see report p. 15***

*"Section 36 sets out the suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects required in connection with the processing of personal data under both Section 42 and Section 54. It provides that such measures may be identified in regulations and may include any of the following: explicit consent, limitations on access to the data within a workplace, time limits for the erasure of the data, targeted training, and, having regard to the 'state of the art', the context, nature, scope and purposes of data processing and the likelihood and severity of risk to the rights and freedoms of data subjects: logging mechanisms; designation of a data protection officer; where the processing involves data relating to the health of a data subject, a requirement that the processing is undertaken by a health practitioner, or a person owing an equivalent duty of confidentiality to the data subjects; pseudonymisation; or encryption. In addition to requiring the putting in place of any such measures, regulations made under Section 36 may also require that governance structures, processes or procedures for risk assessment and for the management and conduct of research projects and other technical and organisational measures designed to ensure that the processing is carried out in accordance with the GDPR together with processes for testing and evaluating their effectiveness be put into effect.*
*The proposed 2018 Regulations will be made under Section 36. The Minister for Justice said at the Report Stage of the Bill in the Seanad (22 March 2018), that the 'toolbox' of safeguards [in Section 36] is 'in addition to, and not a substitute for, the technical organisational measures required under a risk-based approach in Article 24'. "*

***Greece[119] - see report p. 10***

*"The Greek Bill implementing the GDPR does not provide for an authorisation procedure. According to Article 13 of the Bill, the DPA may only be consulted in the following cases: a) where processing of health data and genetic data is carried out on a large scale for purposes in the public interest, such as electronic prescription systems, electronic patient files or health smart cards; b) where health data is processed on a large scale for the purposes of the management of health and social security systems and services; c) for the systematic processing of genetic or biometric data at a large scale."*

***Belgium[120] – see report p. 13***

*Data communicated to the further controller is pseudonymised by the initial controller, who keeps the pseudonymisation key.*

There are a variety of possible safeguards to be implemented to prevent or reduce risks to data subjects' rights and freedoms.

[117] Cf. Doc. 17. Italian legal framework, p. 17.

[118] Cf. Doc 16. Irish legal framework, p. 16.

[119] Cf. Doc. 14. Greek legal framework, p. 12.

[120] Cf. Doc. 04. Belgian legal framework, p. 15.



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

Under the GDPR, while processing for scientific research purposes is specifically addressed at the European level, it still requires a secondary basis, either in national legislation, or another EU legislation. Consequently, national legislations still play a crucial role to define the rules applying to scientific research. Furthermore, other open clauses in the GDPR foster a renewed differentiated regime across Europe, in particular for data subjects' rights. Finally, as under the Directive, national safeguards remain a key element of the regime. While the GDPR prescribes some, Member States retain the possibility to further legislate, in particular concerning the processing of health data, and thus implementing additional safeguards.

Rules applying to processing of health data for scientific research purposes remain complex and differentiated across the EU.

# 5. The framework applied to the research using the AEGLE platform

This section proposes a general normative frame, based on the system described above, for a research team to comply with its data protection obligations when designing a project based on data analytics concerning health, which includes the use of a Big Data analytics platform. The following steps take into account projects based on different categories of data, including identifying and sensitive data, but also the possibility that data may be originating from different countries.

- **Determination of the purpose and modalities of the processing**

At the start of the project, **its purpose**, the nature of the data necessary for the research purpose, as well as the **means of processing**, must be determined by the researchers. The determination of those elements makes the research team and or research sponsors the 'controller' in data protection terms. The notion of controller is defined in the GDPR as "*the natural or legal person, […], determines the purposes and means of the processing of personal data; […]*". For AEGLE, it is clearly the institution sponsoring the research or the research team who defines the purposes of the processing, and decide to use the platform as a tool, or means to achieve such a purpose.

The determination of the legal grounds for the processing is influenced by the nature of the processed data. In the case of scientific research in the field of health, when the processed data includes health and genetic data, there are only a few options. **Either the data is collected specifically for the project on the basis of consent, or the processing is re-use of data based either on consent or on a dual basis found in the GDPR and national law, or EU law**. In the case of the **re-use of data** for scientific research purposes, also the **compatibility** of purpose is presumed, researchers must be mindful of the original processing legal base. In turn, the determination of the legal base of the processing influences the modalities of processing for the controller's obligations; in particular concerning data subjects' information and gathering of their consent.

The controller's obligations are laid out in the GDPR, but in the case of the processing of data concerning health or genetic data, such as scientific research in the health field, **national legislation may provide additional requirements**. Some of the obligations indicated here have been briefly addressed earlier, as part of the necessary safeguards that the controller must implement. However, very often obligations imposed on the controller by the GDPR **coincide with the research and medical practice standards**. Therefore, they will have only little effect on processing for scientific research or medical purposes compliant with standards of the field. Nonetheless, such obligations should be formally integrated into the applicable protocol when possible and complied with.

The researchers must be able to **demonstrate general compliance** with the principles of data processing. This general accountability requires that the researchers document the decisions and action taken. This is why 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

**decisions made by the controller should be documented alongside the research protocol, even when they are made at a later stage of the project**. This documentation must be stored to justify each decision made in case of a supervisory authority inspection. This is a requirement in some Member States (i.e. Belgium). As noted above, this type of information may also be relevant to the research project itself, such as why was it decided that a data set was no longer relevant for the specified purpose.

- **Privacy by design and by default**

**Data protection must be ensured by the design of the research project**, this is the principle of data protection by design.[121] Data protection must also be ensured by default, in the way that only the data necessary for the project is processed.[122] These two principles ensure that the rights and interest of the data subject are taken into account from the start of the processing activity, and that their respect will be included in the default settings of the processing. This means that **privacy must be considered at every stage of the processing**, from the start to the conclusion and that privacy must be respected without the user's intervention. However, the measures implementing these two principles must be **proportional** to the costs and the available techniques, and also account for the nature, scope, context and purposes of the processing.

In practice, this means that privacy is a constant at each stage of the project. Respecting the principles of privacy by design and default are an overarching obligation for controllers, and it has practical consequences for all other obligations. It would be a good practice for a research project to identify early on the security measures to implement and ensure a periodic review and update. Such measures must be included in the records of processing activities. Furthermore, having an adequate data processing policy clearly identifying acceptable practices and ensuring the research protocol is in line with it would be a good way to demonstrate compliance.

- **Designation of Data Protection Officer**

The appointment of a Data Protection Officer (DPO) is a crucial step when one is not already in place, because the **DPO is involved in many decisions taken by the controlle**r. However, the obligation to appoint a DPO does not apply to each research project in particular, but to the institution sponsoring the research in general. The DPO must be consulted at different stages of a project, to ensure compliance with the applicable data protection rules, should be the organisation's DPO. It is nonetheless **advisable that the person in charge of the project should be trained, or at least aware of, the issues relating to data protection**.

The conditions concerning the DPO's appointment depend on the processing activities.[123] The main criteria is that the controller's core activities must be the large scale processing of special categories of data.[124] In this situation, core activities must be understood as key operations for achieving the controller's or the processor's goal, which is the case for scientific research. However, this should not be interpreted as excluding the activities where the processing of data forms an inextricable part of the controller's or processor's activity.[125] Moreover, a number of Member States have set the appointment of a DPO as a requirement of their NDPA.

- **Recruitment of a processor**

[121] Article 25(1) GDPR.

[122] Article 25(2) GDPR.

[123] Article 37 GDPR.

[124] Article 37(1)(b) GDPR.

[125] Article 29 Working Party; WP 243_rev_01, p. 7.



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 use of a data analytics platform is considered as the "recruitment of a processor".[126] A processor in data protection terminology is "a natural or legal person processing personal data on behalf of the controller".[127] The processing by the processor can only happen on the **explicit instruction of the controller** and on the basis of a **data processing agreement** concluded between the controller and the processor.[128] The use of a data analytics platform, such as AEGLE, by a team of researchers must be adequately documented as it is particularly relevant to some of the controller's obligations. For instance, the use of such a tool must be taken into account when a Data Processing Impact Assessment is performed (see below), or when the project is the object of an ethics check.

- **Records of the processing activities**

An important aspect of the accountability principle is the controller's obligation to **maintain a record** of the processing activities. Article 30 GDPR sets out as a requirement that the controller should keep a record of its processing activities. It should also be used by the controller as an opportunity to assess and define clearly before the processing and the collection begin about which data will be necessary for what purpose. **This record should be built when the research protocol is drafted**, to ensure a certain synergy between the two documents.

This obligation has **long term implications**. These records must be kept up-to-date throughout the project and be an accurate reflection of the processing activities.

- **Data Processing Impact Assessment**

Researchers may be required to perform a Data Processing Impact Assessment (DPIA). While the notion of a DPIA is not explicitly defined in the GDPR,[129] the Article 29 Working Party has defined it as a "*process for building and demonstrating compliance*". More specifically: "*DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them*".[130] The DPIA had also been defined in more technical terms by the Commission in 2014 as "*a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes to be carried out by the controller or processor or the processor acting on the controller's behalf*".[131] **The GDPR requires a DPIA to be carried out for the large scale processing of special categories of data and when such processing is likely to result in high risks for the data subject**. This would apply typically to medical research. But as indicated earlier, in case of doubt it is recommended to perform of DPIA. Additionally, when a DPIA is conducted there is an obligation for the processor to support the controller in making the DPIA.

Once the DPIA has been performed, if the results indicate high risks for the rights and fundamental freedoms of the data subjects, then the **competent supervisory authority must be consulted prior to the processing**. For this obligation, there are specificities depending on the countries involved. Sometimes the DPIA's results must be communicated to the data protection authorities, regardless of whether they show risks for the data subjects' rights

[126] Article 28 GDPR.

[127] Article 4(8) GDPR.

[128] Article 28(3) GDPR.

[129] Article 35(7) and Recital 84 GDPR.

[130] Article 29 working party, WP248 rev.01, ; p. 4.

[131] 2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, http://data.europa.eu/eli/reco/2014/724/oj.



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

and freedom. This is one of the opportunities given to the Member States by the GDPR to regulate more specifically and provide additional safeguards.

- **The security of the processing and the notification of personal breach**

The controller must ensure the security of the data and the safety of the processing. This happens through the **adoption of adequate and proportionate security measures**.[132] The measures include, among others: pseudonymisation, encryption, assurance of confidentiality, integrity, availability and resilience of the systems' ability to restore availability and access to the data in the event of an incident, and regular tests and evaluation of the procedures to maintain an up-to-date security system.

Measures adopted can be evaluated based on the DPIA's results, to ensure that, while adequately protecting the data and the data subjects, the security measures do not unnecessarily and unduly hinder the processing. In the event of a data breach entailing risks for the rights and freedom of natural persons, the controller must notify the competent supervisory authority. If the risks caused to the fundamental rights and freedom of the data subjects are high, then the data subjects must be informed as well. The controller must be supported by its processor in such a situation. These obligations may be completed by additional rules over time. They are the **responsibility of the controller**; however, for some of them the **support of the processor** might be required.

- **Compliance with national safeguards**

These are aspects of the processing that must be documented, and once they are all addressed, the collection and the processing of the data may begin. If the research project is based on the re-use of data, then various elements will be needed when applying for access to data sets. Moreover, as seen above, the processing of data concerning health and genetic data may be the object of specific safeguards in the Member State; and compliance with the GDPR obligation may provide a good basis for demonstrating the fairness and safety of the processing. Compliance with national safeguards might prove **problematic for multinational research projects**, or projects relying on data from different countries. Researchers must keep abreast of all national specificities. This is why before engaging in any national formalities that may be required, project sponsors or coordinators should make sure that all European but also national requirements are met.

The concrete application of the regime identified in this legal assessment is done must be done in stages. The implementation of these different stages, identified above, may be complicated by national specificities. This is why clearly mapping out which data will be used and how it will be obtained is essential as it will set the tone of the processing.

# 6. Conclusion

This deliverable has set out to determine the rules applying to the use and reuse of data concerning health for scientific research purposes. It is important to note that many aspects of the depicted regime stem not form the purposes of the processing but from the nature of the data. Therefore many safeguards implemented in the situation of processing for scientific research purposes would be applied in the case of processing for medical and therapeutic purposes as well. To determine the applicable rules, the regimes of thirty European countries have been assessed,

[132] Useful information in that regard can be found in various guidelines and standards on the performance of a DPIA, such as the CNIL's Guidelines, in particular *Privacy Impact Assessment (PIA) 3: Knowledge bases*, the Article 29's working Party Guidelines (WP 248 rev.01), or *ISO's International Standards on Information technology – Security techniques – Guidelines for privacy impact assessment* (ISO/IEC 29134).



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 twenty-eight EU Member States, plus Switzerland and Norway. This evaluation has taken into account the change of legislation that happened in May 2018, and the consequences that has had on national legal frameworks. However, changes of legislation remain pending in many countries and the national reports annexed to this document are often based on draft Bills.

While the European legal framework appears to be harmonised under the GDPR, in practice, national differences remain, due to the GDPR's open clauses. While the GDPR provides for a legal ground for scientific research purposes, this legal ground requires a secondary ground in national legislation or another piece of European legislation and will need to incorporate the application of ethics. Certain data subjects' rights may be derogated if so provided by national legislation and the Member States may implement additional safeguards, conditions or limitations for the processing of health and genetic data. The GDPR establishes relative certainty concerning the applicable legal grounds, but national legislation remains extremely relevant. The main result of the legal assessment is that the **GDPR has not established a fully-harmonised framework for the processing of health data for scientific research purposes** and such a framework would not be legally possible given that allowance needs to be made for national legislations. There may be the potential for an ethical framework that is harmonised. However, the European legislation sets out basic principles applying to all processing activities, and a framework for scientific research. But the content of this framework is determined by national legislation, which determines key aspects of the modalities for scientific research.

This legal assessment has described the European framework and has indicated the points affected by national legislation. The GDPR and national legislation are equally relevant in determining the rules to be applied to any specific project **The basic principle of data processing set out in the GDPR must be applied while national legislation organises the more technical aspects that aim to safeguard data subjects' rights and freedoms**.

Privacy must be considered at each stage of a research project, and many of the researcher's decisions, in terms of the data protection action and results, must be taken at the start of a project. When determining the data used for the project, researchers must be able to answer questions about the data needed and the reason why the legal base will be used for the processing and what will the means of processing be. This is crucial for projects reusing data, where the possible margin of manoeuvre is limited. The selection of the data needed, and the data reused is fundamental. Researchers may derogate data subjects' rights in certain countries if their exercise would significantly and negatively impact upon the research project. As a result, researchers must determine if the data subject's information is feasible. This will be influenced by the pseudonymised or non-pseudonymised character of the data. The researcher must also determine what would be the impact on the research project of data subjects' requests concerning: access, rectification of the data and objection to the processing, and how they would address those requests. The researcher must also determine from the outset of the project what would be the technical and organisational measures to take to ensure the processing's security and safety. The researcher must also determine whether a DPO must be appointed and if a DPIA should be carried out. Answering these questions at the outset of a research project puts the researcher on the right track to comply with data protection law requirements.



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

# Bibliography

***Literature:***

[1] Kitchin, Rob and McArdle Gavin, "What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets; big Data & Society"; January-June 2016; pp 1-10, p.2.

[2] Chassang Gauthier, "The impact of the EU general data protection regulation on scientific research", *ecancermedicalscience*, 2017

[3] Rumbold John Mark Michael and Barbara Pierscionek, "The Effect of the General Data Protection Regulation on Medical", *Journal of Medical Internet Research,* vol.19(2), 2017.

[4] Matthieu Bourgeois, « Droit de la Donnée : Principes théoriques et approche pratique », *Lexis Nexis* ; 2017

[5] Information Commissioner's Office, "ICO's Big data, artificial intelligence, machine learning and data protection" version 2.2, 2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[6] Commission de la protection de la vie privée, Frank De Smet assisted by Cliff Beeckman and Dieter Verhaeghe, « Rapport Big Data », 2017, https://www.autoriteprotectiondonnees.be/node/20757

[7] European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, 2003

[8] European Commission, "Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, 2014/724/EU", 2014, http://data.europa.eu/eli/reco/2014/724/oj.

***Artilce 29' Working Party : Opinions and Guidelines:***

[9] Article 29's Working Party, WP187 , Opinion 15/2011 on the definition of consent, 2011

[10] Article 29's working party, "WP 203, Opinion 03/2013 on purpose limitation", 2 April 2013

[11] Article 29's Working Party, "WP259 Guidelines on Consent under Regulation 2016/679", 2017

[12] Article 29's Working Party, "WP 243 rev. 01, Guidelines on Data Protection Officers", 2017

[13] Article 29's working party, "WP248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 2017

[14] Article 29's working party, " WP 260 rev.01Guidelines on transparency under Regulation 2016/679", 2018

[15] European Data Protection Supervisor, "Opinion 7/2015, Meeting the Challenges of Big Data, A call for transparency, user control, data protection by design and accountability", 19 November 2015



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

***Legislation:***

[16] Regulation (EU) 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) (Text with EEA relevance)

[17] 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

# Abbreviations

- DoW: Description of Work
- HW, H/W: Hardware
- SW, S/W: Software
- DPD Data Protection Directive
- GDPR: General Data Protection Regulation
- EU: European Union
- DPO: Data Protection Officer
- DPIA: Data Processing Impact Assessment
- DPA: Data Protection Act
- NDPA: New Data Protection Act

### *Country codes:*

**Table 1: Country Codes (Eurostat)[133]**

| COUNTRY | CODE | COUNTRY | CODE | COUNTRY | CODE | COUNTRY | CODE |
|---|---|---|---|---|---|---|---|
| Belgium | (BE) | Greece | (EL) | Lithuania | (LT) | Portugal | (PT) |
| Bulgaria | (BG) | Spain | (ES) | Luxembourg | (LU) | Romania | (RO) |
| Czech Republic | (CZ) | France | (FR) | Hungary | (HU) | Slovenia | (SI) |
| Denmark | (DK) | Croatia | (HR) | Malta | (MT) | Slovakia | (SK) |
| Germany | (DE) | Italy | (IT) | Netherlands | (NL) | Finland | (FI) |
| Estonia | (EE) | Cyprus | (CY) | Austria | (AT) | Sweden | (SE) |
| Ireland | (IE) | Latvia | (LV) | Poland | (PL) | United Kingdom | (UK) |
| Norway | (NO) | Switzerland | (CH) | | | | |

[133] http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Country_codes



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

# Appendix A. Table: Different categories of safeguards and the countries in which there are implemented

| Categories of safeguards | Explanation | Concerned countries |
|---|---|---|
| Supervision by a health professional | Stated in the Directive. | BE, CY, IE, LT, SK |
| Professional secrecy | Statutory/contractual obligation. | **ALL BUT** DK, EE, FI, DE, EL, CH |
| Encryption | Encryption (pseudonymised) is favoured. Means that processing of coded data should be favoured over fully-identifiable data. | **ALL BUT** BG, HR, CY, CZ, DK, FI, DE, LU, MT, SK, SI |
| Authorisation DPA | The data protection authority authorises the processing of special categories of data. | **ALL BUT** HR, CZ, HU, IE, PL, SI, SK |
| Important public interest | More than just public interest (as stated in the Directive). | AT, IT, LV, PT |
| Agreement of initial controller | In the case of further processing. | AT, BE, HU, SK |
| Administrative obligation/requirements | Requirement set for the authorisation, information is to be provided for the authorisation:<br>Identity of person processing, demonstration of the aptitude of the controller. | AT, BE, FI, FR, DE, EL, HU, PT, CH |
| Ethics committee approval | Ethics approval is required in the case of interventional studies (when the data is collected for the purpose of a study) some countries require it also when data is collected from a third party (ethics of the project in general). | **ALL BUT** HR, CZ, LV, PL, RO |
| Technical and organisational measure for security | The processing of data must follow relevant protocols, and adequate security measures must be implemented by the controller. | **ALL BUT** CZ, DK, MT, RO, SI |
| Necessity of the processing | The processing of the personal data concerned must be necessary for the research project. | IE, PT, SE, CH |
| After processing data is anonymised | Some countries require the data to be fully depersonalised after it is no longer necessary for the research. | AT, CY; FI, DE, HU, LT |
| Data processed exclusively for scientific research purpose | The controller may only process data for scientific purposes. | DE, EL, HU |
| Specific requirement for specific categories | The regime applying to genetic data can be different, especially since genetic data is not defined as a special category of data by the Directive. | IT, ES, CH |

In darker gray, areas to still pay attention to under the GDPR



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

# Appendix B. List of country reports

| Country | Author(s) | Last version | Name of the document |
|---|---|---|---|
| Austria (AT) | Max Mosing and Juliane Messner | 17/07/2018 | 03. Austrian legal framework |
| Belgium (BE) | Mahault Piéchaud Boura | 23/08/2018 | 04. Belgian legal framework |
| Bulgaria (BG) | Desislava Krusteva and Silvena Rakshieva | 23/07/2018 | 05. Bulgarian legal framework |
| Croatia (HR) | Boris Dvoršćak | 04/04/2018 | 06. Croatian legal framework |
| Cyprus (CY) | Olga Georgiades | 02/05/2018 | 07. Cyprus's legal framework |
| Czech Republic (CZ) | Zdeněk Kučera and Matouš Michal | 02/05/2018 | 08. Czech legal framework |
| Denmark (DK) | Mette Hartlev | 25/06/2018 | 09. Danish legal framework |
| Estonia (EE) | Cathriin Torop | 19/04/2018 | 10. Estonian legal framework |
| Finland (FI) | Peter Hanninen | 08/05/2018 | 11. Finnish legal framework |
| France (FR) | Mahault Piéchaud Boura | 08/08/2018 | 12. French legal framework |
| Germany (DE) | Stefanie Hänold, Friederike Knoke and Tina Krügel | 30/04/2018 | 13. German legal framework |
| Greece (EL) | Ioannis Iglezakis | 02/04/2018 | 14. Greek legal framework |
| Hungary (HU) | András Jóri, Andrea Soós and Katalin Horváth-Egri. | 20/08/2018 | 15. Hungarian legal framework |
| Ireland (IE) | Maeve McDonagh and Mary Donnelly | 12/06/2018 | 16. Irish legal framework |
| Italy (IT | Raffaella Cesareo | 30/03/2018 | 17. Italian legal framework |
| Latvia (LV) | Valts Nerets | 25/07/2018 | 18. Latvian legal framework |
| Lithuania (LT) | Sidas Sokolovas | 05/04/2018 | 19. Lithuanian legal framework |
| Luxembourg (LU) | Mahault Piéchaud Boura | 28/08/2018 | 20. Luxembourg's legal framework |
| Malta (MT) | Philip Mifsud | 27/07/2018 | 21. Maltese legal framework |



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

| | | | |
|---|---|---|---|
| Norway (NO) | Emily Mary Weitzenboeck and Line Coll | 23/07/2018 | 22. Norwegian legal framework |
| Poland (PL) | Dariusz Adamski | 05/06/2018 | 23. Polish legal framework |
| Portugal (PT) | Antonio Borges | 23/04/2018 | 24. Portuguese legal framework |
| Romania (RO) | Magda Alexandru | 30/07/2018 | 25. Romanian legal framework |
| Slovakia (SK) | Zuzana Halasova | 25/07/2018 | 26. Slovak legal framework |
| Slovenia (SI) | Marko Kranjc | 04/04/2018 | 27. Slovenian legal framework |
| Spain (ES) | Pedro Letai | 18/06/2018 | 28. Spanish legal framework |
| Sweden (SE) | Christine Storr and Pam Storr | 08/04/2018 | 29. Swedish legal framework |
| Switzerland (CH) | Florent Thouvenin and Damian George | 05/06/2018 | 30. Swiss legal framework |
| The Netherlands (NL) | Evert-Ben van Veen | 23/05/2018 | 31. Dutch legal framework |
| United Kingdom (UK) | Ian Lloyd | 06/04/2018 | 32. British legal framework |



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

# Appendix C. List of additional documents

- Research protocol : Doc. 02. Research protocol, drafted in February 2018 for legal experts providing national input for all EU countries , Norway and Switzerland.



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