Report on Legal framework in EU
<table>
<thead>
<tr>
<th><strong>GRANT AGREEMENT NUMBER 824666</strong></th>
<th><strong>ACRONYM: FAIR4Health</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full title</strong></td>
<td>Improving Health Research in EU through FAIR Data</td>
</tr>
<tr>
<td><strong>Horizon 2020 Call</strong></td>
<td>SwafS-04-2018: Encouraging the re-use of research data generated by publically funded research projects</td>
</tr>
<tr>
<td><strong>Type of action</strong></td>
<td>Research and Innovation Action</td>
</tr>
<tr>
<td><strong>Start Date</strong></td>
<td>1st December 2018</td>
</tr>
<tr>
<td><strong>Website</strong></td>
<td><a href="http://www.fair4health.eu">www.fair4health.eu</a></td>
</tr>
<tr>
<td><strong>Project Officer</strong></td>
<td>Raluca Iagher</td>
</tr>
<tr>
<td><strong>Project Coordinator</strong></td>
<td>Carlos Luis Parra Calderón, Andalusian Health Service</td>
</tr>
<tr>
<td><strong>Related task</strong></td>
<td>D.2.3. Guidelines for implementing FAIR open data policy in health research</td>
</tr>
<tr>
<td><strong>Release date</strong></td>
<td>May 2019</td>
</tr>
<tr>
<td><strong>Dissemination Level</strong></td>
<td>Public</td>
</tr>
<tr>
<td><strong>Responsible Author</strong></td>
<td>Carlos Rapallo Fernández</td>
</tr>
<tr>
<td><strong>e-mail</strong></td>
<td><a href="mailto:Carlos.Rapallo@garrigues.com">Carlos.Rapallo@garrigues.com</a></td>
</tr>
<tr>
<td><strong>Collaborators</strong></td>
<td>Matias Garrido Cortés - Carlos Crespo Correro</td>
</tr>
<tr>
<td><strong>Keywords</strong></td>
<td>Guidelines, FAIRdata, legal issues</td>
</tr>
</tbody>
</table>
Table of Contents

1. Legal framework in EU .............................................................................................................. 2
  1.1. Introduction ................................................................................................................................. 2
  1.2. Legislation analyzed ..................................................................................................................... 2
      1.2.1. Regulations .......................................................................................................................... 2
      1.2.2. Principles of interpretation ................................................................................................. 3
      1.2.3. Concept of data under Fair4Health Project ...................................................................... 9
      1.2.4. Legal requirements ............................................................................................................ 10

Annex I. Executive summary of National Regulations ................................................................. 26
1. Legal framework in EU

1.1. Introduction

The analysis of the impact of GDPR and national regulations in EU on FAIR open data policy implementation in Health research is key to the success of Fair4Health.

To ensure the success of Fair4Health it will be analysed the concept of personal data and data within the framework of research and Fair4Health as well as the analysis of the requirements that according to the GDPR and national regulations must fulfil the data for their access to the platform, as well as the responsibilities of the members as responsible for the processing of personal data.

All the aspects regarding the legal aspects of the functioning of FAIR4Health’s platform are developed in the deliverable D.2.2. “Functional design of the FAIRification tool-FAIRification workflow”.

1.2. Legislation analyzed

For the purpose of this study, the EU implementing legislation has been analysed. The study is based on the General Data Protection Regulation (GDPR) since it will be generally applicable to all members, so in case the national legislation of the members contradicts the GDPR will prevail the GDPR. A table reflecting the implementing regulations of the members is attached as Annex A.

1.2.1. Regulations

1.2.1.1. EU


1.2.1.2. National Regulations

In accordance with task T2.4. of the project, the national regulations analysed are Italian, Serbian, Spanish and Swiss.

❖ Italy. Legislative Decree no. 196 of 30 June 2003, containing the "Code for the protection of personal data".
https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezion e+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.6

❖ Italy. General authorization n. 9/2016 to process personal data for scientific research purposes, 15 December 2016;
1.2.2. Principles of interpretation

Due to the importance of the GDPR it is considered necessary to attend to the importance of the following GDPR’s Whereas, that helps to interpret its content:

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration
the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or
Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those
purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(65) A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not
fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of
life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union’s objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

The Article 29 Working Party ("WP29") is the independent European working group that has dealt with issues related to the protection of privacy and personal data until 25 May 2018 (entry into force of the GDPR). The Article 29 Data Protection Working Party was composed of:

- **a representative of the supervisory authority (ies)** designated by each EU country;
- **a representative of the authority (ies)** established for the EU institutions and bodies;
- **a representative of the European Commission.**

Due to the importance of the work of the WP29 for the interpretation of the GDPR it is considered necessary to pay attention to the interpretation given in their Opinions and Guidelines mentioned below:

1.2.3. Concept of data under Fair4Health Project

Article 4 GDPR contains the definitions that are of particular interest in the framework of the GDPR. For the purposes of the Fair4Health Project, it is essential to define the concept of personal data and health data in accordance with what is established by EU legislation, since this will be the general legislation applicable to all members due to the direct effectiveness that the GDPR brings with it.

1.2.3.1. Personal data

According to Article 4.1 GDPR, “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

The GDPR is precise when states that any data about a natural person is considered personal data. It is true that, as it is analysed later on, it is possible to identify special categories of personal data, but as far as the concept of personal data is concerned the GDPR is short and concise. Thanks to the consideration that all data related to a natural person’s personal data will enjoy the special protection guaranteed by the GDPR.

1.2.3.2. Health data

The GDPR distinguishes between ‘data concerning health’ and ‘genetic data’. For the purposes of this paper, both definitions are of our interest:

- ‘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” (Article 4.15).
- ‘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” (Article 4.13).

Both concepts, for the purposes of this document, will be jointly hereafter referred as “health data”.

1.2.3.3. Fair4Health Data
After a first approach to the concept of health data through the definitions included in the GDPR, it is essential to include the aforementioned personal data within the framework of the Fair4Health Project.

Therefore, 'Fair4Health Data' means health data, meeting the requirements of anonymisation and/or pseudonymisation, to be shared in the platform for means of biomedical investigation. These Fair4Health Data shall also fulfil some other requirements such as consent, transfer of data, re-use or modification as it is referred later on.

1.2.3.4. FAIRify

To be more specific when talking about data related to Fair4Health Project, we would distinguish the concept of "FAIRify" as what the members shall do with the Fair4Health Data.

Therefore, when talking about ‘FAIRify’ it means “to translate raw (meta) data into Findable, Accessible, Interoperable and Reusable (meta) data according to the FAIR data guiding principles”.

1.2.4. Legal requirements

The Fair4Health Project is a scientific research project, in particular biomedical. The platform aims to share personal data related to health for the development of research. To this end, the members, as controllers, will be in charge to FAIRify personal, health and medical data into Fair4Health Data in order to re-use health data generated by previous research projects or specifically collected for research purposes by the members.

Article 9.1 of the GDPR creates a distinction between personal data and special categories of personal data. This article starts from the general principle of the prohibition of processing such data, stating that "The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data intended to uniquely identify a natural person, data relating to health or data relating to the sexual life or sexual orientation of a natural person shall be prohibited". Therefore, processing Fair4Health data, as personal data concerning health, shall be prohibited according to Article 9.1 GDPR.

However, this principle is exempted in the cases listed in Article 9.2, being particularly relevant for the purposes referred in points (a) and (j), which legitimize such processing when:

(a)  "data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide

---

1 In order not to have the consideration of personal data, Fair4Health Data must be anonymous, however this is impossible when it comes to personal data related to health as it is set out in section 4.2.4.2. of this report dedicated to the “Anonymisation and/or pseudonymisation”.
that the prohibition referred to in paragraph 1 may not be lifted by the data subject”;
and

(j) “processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.

It is important to point out that the members will have to comply, unavoidably, as controllers with the information rights of the data subject contained in Articles 13 and 14 GDPR.

Where personal data are directly obtained from the data subject, members must comply with the obligations set out in Article 13 GDPR, and provide the data subject with all of the following information:

(a) “the identity and the contact details of the controller and, where applicable, of the controller’s representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.”

According to Article 13.2 GDPR “the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.”

And last, Article 13.3 GDPR states that "where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2”.

Article 13 GDPR shall be taken into account by the members as controllers when supplying health data to the Fair4Health platform. However, once on the platform it will be necessary for the members to take into account the obligations established by Article 14 GDPR when they are going to process Fair4Health Data obtained from the platform directly.

Exceptionally, it shall not be necessary to comply with this obligation in accordance with point 5 of Article 14, which states that “paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available;”

Aside from the information right, it will now proceed to develop the necessary requirements for FAIRify personal data in Fair4Health Data.

1.2.4.1. Consent
a) Scenarios

Within the framework of the Fair4Health project it will be necessary for the data subject to give her/his consent to be able to FAIRify personal data in order to provide those data to the platform for the development of scientific research.

As a general rule, the processing of this category of personal data is prohibited; however, it is possible to process them if the data subject gives explicit consent, as seen in section 2.4 above. For this reason, it should be understood that as long as it is not under an exception to the general rule, such as the public interest, the prior consent of the interested parties will be necessary for the data to be FAIRified so that they can be processed in biomedical research. This consent may have been given by the data subject for biomedical research in general or specifically.

Frequently it is not possible to fully determine the purpose of the processing of personal data for scientific research purposes at the time of collecting consent. Whereas 33 states that data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Accordingly, it can be distinguished two scenarios in which consent will be required:

1. The first scenario in which it will be necessary to obtain the consent of the data subject for the biomedical research, being able to have this general or specific character. In case the consent is specifically given, it may and must be specified later when it is not possible to fully determine the purpose of processing.

2. The second scenario in which it will not be necessary to obtain consent on several grounds is when the data meet the conditions to be reused that are analysed in the following paragraph 2.4.4.

b) Formal requirements

The first essential requirement is consent. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to her or him, such as by a written statement, including by electronic means, or an oral statement. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Therefore, the data subject must consent to the use of human biological samples for scientific research purposes as well as to the use of clinical data. It will be admitted as consent to tick a box when filling out a form at the time of an analysis or medical test, among others, as long as it is specified that it is generic or for the Fair4Health platform.
Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

Whereas 42 states than “where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given”. For consent to be informed “the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”.

Consent will always be required, whether or not it is anonymized as long as the resulting dataset would still be personal data. Exceptionally, coded or identified samples may be processed for biomedical research purposes without the consent of the data subject where it is possible to re-use them.

Consent may be generic or specific. As far as possible, consent shall preferably be generic so that platform users can make use of the data in research of different types. However, it may be possible for the data subject to give her or his consent in a more specific way: for a specific research or for a type of research (e.g. consent for the processing of data in the framework of cancer research).

The processing of personal data shall be permitted only if the data subject has consented to the processing of his personal data for one or more specific purposes. The members must be able to demonstrate that the data subject consented to the processing of his or her personal data.

In the framework of scientific research and whenever it is necessary in the absence of a reason of public interest that makes consent unnecessary, the data subject may withdraw her/his consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal, and each member, as the data controller, is responsible for withdrawing the data from the platform.

It is true that, as established by WP29 in its Article on Guidelines on consent under Regulation 2016/679, when the data subject withdraws his consent and the controllers must comply, there will be no exception to this requirement in the case of scientific research. However, there are exceptions to the right to erasure and the right to object in case the data subject decides to exercise these rights in a way that even if consent is withdrawn, these data could be processed in the framework of the research of which they form part at that time but not reused, although they should not be erased. This is what follows from Whereas 65 when it states that “the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal
obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims” as well as Article 17.3.(d) GDPR which establishes as an exception to the exercise of the right to erasure the necessary treatment when this is “for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing”. As for the right to object, the exception to the exercise of this right is limited to “the processing is necessary for the performance of a task carried out for reasons of public interest” as set out in Article 21.6 GDPR.

The members must fulfil this requirement in order to FAIRify the personal data.

1.2.4.2. Anonymisation and/or pseudonymisation

As anticipated, according to Opinion 05/2014 on Anonymisation Techniques the advance of technology does not allow a total anonymisation so that the data despite having been anonymised still have the condition of personal data and are therefore subject to data protection regulations for their processing. If, at some point it is possible to achieve total anonymisation that would guarantee the absolute impossibility of re-identifying the data subject, the anonymised data would cease to have the status of personal data and could be processed without the need to comply with the data protection requirements laid down.

In the framework of this project, it will always be necessary to process anonymised data in accordance with data protection legislation, and in particular the GDPR. Indeed, Article 89 GDPR provides that “technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner”.

Although the GDPR makes direct reference only to pseudonymisation, it does not mean that other measures to ensure the principle of data minimisation are excluded. In this sense, Whereas 28 states that “The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.”

Among these measures, the GDPR envisages the possibility of resorting to pseudonymisation but other measures could be considered if fulfilling the necessary requirement that is to achieve the minimisation of personal data in such a way that the identification of data subjects is not possible.
Both processes of pseudonymisation and anonymisation pursue the objective of minimizing personal data in order to avoid the identification of the data subject. However, the anonymisation process is more restrictive than the pseudonymisation process as the latter allows by means of additional information to identify the subject.

The process of anonymisation and pseudonymisation are compatible with the use of the platform. The need to resort to one process or the other will depend on the national regulations of the members, since for the purposes of the platform the fundamental thing is that it is not possible to identify the data subject. In the case of pseudonymisation, the members as data controllers must guarantee that the additional information that allows the identification of the data subject is not accessible to any user of the platform. Therefore, in order to have a better understanding of the scope of these measures it will proceed as follows to analyse them separately.

a) Pseudonymisation

(i). Concept

Article 4.5 GDPR gives the definition of the pseudonymisation stating that pseudonymisation “means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information shall be kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

(ii). Limitation to the use of pseudonymised data

Article 25 GDPR states in its first paragraph that “taking 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 of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects”. In its second paragraph, it continues that “the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons”.

The use of pseudonymisation as a measure to comply with the principle of data minimisation is limited to compliance with the regulations of the Member States.
referred to in Annex A accompanying this report. National laws may establish more restrictive measures than pseudonymisation, such as anonymisation, in which case it will not be possible to use this measure to comply with the principle of minimisation. On the contrary, as long as the national laws do not pronounce on the matter or require that the measures to comply with the principle of data minimisation be less restrictive or equal to pseudonymisation, it will be possible to resort to this measure.

It must not be forgotten that, although the GDPR refers to pseudonymisation as a measure, it does not require the person responsible for minimising data to go to this procedure which may resort to any procedure which complies with the aforementioned principle.

b) Anonymisation

(i). Concept

Data anonymisation is a process consisting of eliminating or minimising the risks of re-identification of anonymised data while maintaining the veracity of the results of the processing thereof, i.e. in addition to avoiding the identification of individuals, anonymised data must guarantee that any operation or processing carried out after anonymisation does not lead to a distortion of the actual data.

GDPR does not give a proper definition of anonymisation although Whereas 26 understands anonymous data to mean “information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”, so that data protection principles do not apply to anonymous information.

The WP29 in its Opinion 05/2015 interprets Whereas 26 of Directive 95/46/EC as regards anonymisation in terms similar to GDPR stating that “data must be processed in such a way that it can no longer be used to identify a natural person by using “all the means likely reasonably to be used” by either the controller or a third party. An important factor is that the processing must be irreversible”.

It should be recalled here that anonymisation is also defined in international standards such as the ISO 29100 one – being the “Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party” (ISO 29100:2011). Irreversibility of the alteration undergone by personal data to enable direct or indirect identification is the key also for ISO.

(ii). Problematics of absolute anonymisation

Once the concept of anonymisation has been determined, it is necessary to tackle the problem that prevents complete anonymisation. In order to do so, it will be
necessary to fully understand the anonymisation process and to evaluate the risks and impediments, as well as to establish in which cases anonymous data can be considered totally anonymised and therefore lose the personal data character.

Considering that anonymisation is a technique applied to personal data in order to achieve irreversible de-identification, the starting assumption is that the personal data must have been collected and processed in compliance with the applicable legislation on the retention of data in an identifiable format.

Anonymisation may be a good strategy to keep the benefits and to mitigate the risks. Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. However, it is clear from case studies and research publications that the creation of a truly anonymous dataset from a rich set of personal data, whilst retaining as much of the underlying information as required for the task, is not a simple proposition. For example, a dataset considered to be anonymous may be combined with another dataset in such a way that one or more individuals can be identified\(^2\).

The purpose of the anonymisation process is to eliminate or reduce to a minimum the risks of re-identification of the anonymized data while maintaining the veracity of the results of the data treated. Besides avoiding the identification of persons, the anonymized data must guarantee any operation or treatment that may be carried out after anonymisation does not lead to a distortion of the real data.

However, this is not so simple, as absolute anonymisation of the data cannot be guaranteed. For this reason, in the anonymisation process, it is essential to assess the risks of re-identification a posteriori and how the confidentiality of anonymized personal information will be guaranteed. Among other requirements established by law, it is the duty to guarantee the clear separation of the data so that the anonymized data of the original data do not coincide in the same person, avoiding their identification.

In accordance with the foregoing, the process of anonymisation shall result in the breaking of the chain of identification of persons. This chain consists of microdata or direct identification data and indirect identification data. The microdata allows the direct identification of persons and the indirect identification data are crossed from the same or from different sources that may allow the de-identification of persons, such as information from other databases of the same or another person responsible, among others.

For the development of the anonymisation process, it will be necessary to foresee the consequences of a possible re-identification of the persons that could generate a damage or loss of their rights. It will also be necessary to foresee a hypothetical loss of information due to the negligence of the personnel involved, due to the lack of an adequate anonymisation policy or due to an intentional disclosure of secrecy that

\(^2\) Opinion 05/2014 on Anonymisation Techniques, WP216, 0829/14
would result in the loss of the identification variables or identification keys of the persons.

However, as WP29 reminds us, it is essential that as long as the original (identifiable) data are not erased the resulting data will continue to be treated as personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous.

As a general rule, especially in the field of biomedical research as it is a category of special data, it is essential to understand that it is not enough to remove the elements that can be used to directly identify a person in order to ensure that the person concerned can no longer be identified.

WP29 understands that "genetic data profiles are an example of personal data that can be at risk of identification if the sole technique used is the removal of the identity of the donor due to the unique nature of certain profiles. It has already been shown in the literature that the combination of publically available genetic resources (e.g. genealogy registers, obituary, results of search engine queries) and the metadata about DNA donors (time of donation, age, place of residence) can reveal the identity of certain individuals even if that DNA was donated "anonymously"." This example is essential for us to understand the problems presented within the framework of the Fair4Health Project, since the risk of identifying health data is inevitable, so that health data will always be considered as personal data due to the difficulty of guaranteeing their anonymisation in accordance with their special nature. In accordance with the foregoing, despite being anonymised, the data must always be processed in accordance with data protection regulations and their requirements.

(iii). Limitation to the use of anonymised data

In accordance with Article 25 GDPR, the use of anonymisation as a measure to comply with the principle of data minimisation is limited to compliance with the regulations of the Member States referred to in Annex A accompanying this report.

Where national laws provide for anonymisation as a measure for minimising data, there is no doubt about the limitation of the data controller to the use of anonymised data. If this is the case, the data controller should use this measure. However, when the national laws do not say anything about it or do not show a preference it will be possible to resort to this measure.

The limit for the use of anonymisation as a measure will be that national laws will establish a clear, binding preference for another measure or that a more restrictive measure, if possible, will be established than anonymisation. As it has been seen, the GDPR does not have a specific preference, leaving those responsible the decision to opt for one measure instead of another depending on what each Member State establishes.
Anonymisation is the preferred solution, for WP29, if the end of the investigation can be achieved without the processing of personal data.

1.2.4.3. Transfer

a) Concept

First of all, it is fundamental to stop at the free circulation of personal data referred to in Article 1 GDPR: "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

On the other hand, when the GDPR refers to data transfers as "flows of personal data to and from countries outside the Union and international organisations" and considers them that "are necessary for the expansion of international trade and international cooperation" is actually referring to cross-border transfers without actually addressing the transfer of data between Member States or even within the same Member State.

b) Possible scenarios under Fair4Health project

Within the framework of the Fair4Health Project, data transfer can be found in two different scenarios:

(i) The transfer of data from members to the Fair4Health platform for use in the framework of scientific research;

(ii) The transfer of data from the Fair4Health platform to members or third parties in the framework of scientific research.

In any of the scenarios, it will be necessary for the transfer of personal data general compliance with the requirements set out in the GDPR, especially with consent as a fundamental requirement for the processing of personal data. Aside from this, in those cases where members or third parties who are going to agree to process the data are not part of the European Economic Area, they must be based on an adequacy decision (Article 45), by means of adequate safeguards (Article 46) or in the case of specific situations for which certain exceptions are established in the GDPR (Article 49).

c) Requirements

The objective of the EU with the GDPR is to guarantee the protection of personal data and the free circulation of these data. Also, the Fair4Health platform seeks to ensure the flow of data in the field of scientific research.

---

3 Whereas 101, GDPR.
One of the requirements to be met by the members as data controllers is to ensure the transfer of the data in a secure manner and in accordance with the implementing rules such as:

(i) Consent;

(ii) Information;

(iii) Transfer according to guarantees and adequacy.

Regarding consent, in relation to the previously mentioned, it is necessary to obtain consent for the transfer of data, provided that the guarantees established by the regulations or which take place within the EU are complied with.

The controller must inform the supervisory authority and the interested party of the transfer\(^4\). However, this obligation shall not be necessary where, in accordance with Article 14.5. GDPR: “(a) the data subject already has the information” y “(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available”.

Although the project was born within the European Union, the use of the platform is not limited to the European Union but third countries or international organisations may participate in it, either to provide data platform or for use in research. For this reason, it is essential to comply with the GDPR with regard to transfers of personal data, collected in Chapter V.

The members as controllers must comply at least with the conditions laid down by the GDPR including those relating to further transfers of personal data from the third country or international organisation to another third country or another international organisation in case it is applicable to every singular case:

- **Transfers on the basis of an adequacy decision**: where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection the transfer shall not require any specific authorisation.

\(^4\) Whereas 113, GDPR.
- **Transfers subject to appropriate safeguards**: in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46.2 GDPR establishes that the appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure;

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure;

(e) an approved code of conduct with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or

(f) an approved certification mechanism with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

Even though, subject to the authorisation from the competent supervisory authority, the appropriate safeguards may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies, which include enforceable and effective data, subject rights.

1.2.4.4. Re-use

According to the definition of FAIRify, the re-usability of the data is an essential feature that requires that data collected for certain purposes be re-used for a different purpose. The importance of being able to determine under what circumstances such reuse of data collected by members is possible makes reuse one of the requirements for the processing of data for biomedical research purposes in the framework of the Fair4Health project.
The data must be able to be reused for different investigations without altering their essential content. In order to do so, the data subject must have previously given her/his consent for the reuse of the personal data.

The scope of the consent given by the data subject shall be the one determining whether or not such data may be re-used. This implies that where the processing must be based on consent, the data subject should be clearly and unequivocally aware of the purposes for which the processing will be carried out, as it happens in this case.

Personal data may be reused in certain circumstances that are established on the basis of:

(i). Type of consent given: generic or specific;

(ii). Prior/previous processing of data for the purposes for which consent was given;

(iii). The exercise of the rights of opposition, rectification and erasure; and

(iv). Withdrawal of consent.

While Whereas 159 states that "the processing of personal data for scientific research purposes should be interpreted in a broad manner", WP29 in its Guidelines on consent under Regulation 2016/679 considers that "the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice". Therefore, consent will be required provided that the data will be processed in the framework of a different project for which consent was not initially given.

Once the circumstances that must be taken into account when considering whether or not a data is reusable have been determined, it is necessary to analyse the possible scenarios that are detailed below:

(a) The data shall be reusable:

1. Where the data subject has given generic consent for the purpose of scientific and/or biomedical research;

2. In the case of further processing of data for which consent has been given for purposes other than those for which they are intended to be re-used, in which case they may be re-used within the same scientific research despite the fact that the purposes may be different.

The controllers shall inform the data subject if they plan to further process her/his personal data for a purpose other than that for which they were obtained. WP29 also continues to analyse that "these provisions specifically give effect to the principle in Article 5.1(b) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is incompatible with these purposes is prohibited" and that "the
second part of Article 5.1(b) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are compatible with the original purposes (Article 6.4 informs this issue, Articles 13.3 and 14.4 apply).

As regards scientific research, Article 89(1) establishes a general exception to the further processing of data, when the respect of the principle of minimisation of personal data is guaranteed, it states that the purposes will be compatible: “where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner”. Likewise, Whereas 62 establishes, as it has been seen previously, an exception to the obligation to provide information “where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort” which may apply under the Fair4Health Project as long as the consent has been given on a general basis and not within the framework of a specific scientific research.

(b) The data shall not be reusable:

1. Where the data subject has given her or his consent for specified purposes and the data have not been processed;
2. Where the data subject has withdrawn consent, even though the data may not have been deleted;
3. Where the data subject has exercised his rights of objection or withdrawal;
4. When the data have been previously processed but any of the cases collected in cases 2 and 3 above occur, or when the data has been rectified since its last processing and its consent has been given for specific purposes, in which case it would again be faced with case 1.
5. When data processing is planned outside the research project for which consent was originally given.

Whereas 65 considers the exception to the exercise of the right of suppression when it states that “the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims”. 

---

5 Whereas 65 considers the exception to the exercise of the right of suppression when it states that “the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims”. 

---
By virtue of the principle of data minimisation, and of the guarantees that it establishes, it follows from Whereas 156 the possibility of “the further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist”. Accordingly, the reuse of personal data would be possible for different purposes as long as it is in the same scientific research project for which the consent was collected.

Whereas 157 broadens the scope of the investigation taking into account the possible collection of data from registries. It thus recalls that “by coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.”

The Fair4Health platform functions essentially as a record of medical data for research purposes, so it is critical to obtain more consistent results and combine research to make that data reusable.
## Annex A. Executive summary of National Regulations

<table>
<thead>
<tr>
<th>Requirement Country</th>
<th>Consent is mandatory for</th>
<th>Consent’s Withdrawal</th>
<th>Right of information</th>
<th>Anonymisation and/or Pseudonymisation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Processing</td>
<td>Transfer</td>
<td>International transfer</td>
<td>Reuse</td>
</tr>
<tr>
<td>Italy</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serbia</td>
<td>YES</td>
<td>Article 4.12), 12, 15, 17 Law on Personal Data Protection</td>
<td>Article 11 and 36 Law on Personal Data Protection</td>
<td>Article 15 and 30.2) Law on Personal Data Protection</td>
</tr>
<tr>
<td>Country</td>
<td>YES</td>
<td>Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Pseudonymisation 16th additional provision. 2.d) Organic Law 3/2018