EOSC-Pillar

Coordination and Harmonisation of National &Thematic Initiatives to support EOSC

Legal Framework for the use and re-use of health data for scientific purposes

Lead Partner:	INFN
Version:	Final
Status:	Submitted
Dissemination Level:	Public
Document Link:	https://repository.eosc-pillar.eu/index.php/s/7D6RbNtAgq8ZnmS

Document Abstract

Subtask T6.6.4 – “Health data security aspects” concerns Legal and ethics requirements on the storage and handling of health data are becoming stricter (e.g. GDPR). In some cases, legal gaps can create obstacles to data sharing and interoperability. This subtask will look at how proposed solutions can be put in place while meeting those strong security requirements.

This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under grant agreement No. 857650.

COPYRIGHT NOTICE

DELIVERY SLIP

Date	*Name*	*Partner/Activity*	*Date*
From:	Nadina Foggetti	INFN	3/03/2022
From:	Giacinto Donvito	INFN	3/03/2022
From:	Marco Tangaro	CNR-IBIOM	3/03/2022

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v.1			
…			
…			
v.n			

Executive summary

Index:*1. Introduction – 2 The Legal Framework – 2.1 EU Legal Framework: the principles applicable to health data – 2.2 The Regulation in the Italian Law -2.3 The Regulation in France Law – 3. The Application of the EU Regulation: the differences between member state's Legal Order – 4. Legal Bases for the use of Health data in the context of scientific research: the applicability of the OS principles and FAIR Principles – 5. Pseudonymisation and anonymisation– 6. Harmonization of Safeguards for Selected Sectors (e.g., Health, Genetics)– 7 Best Practices for the implementation of Scenario 3.*

1 Introduction

Task 6.6, Use case 6, aims to explore reference data through existing computing services for the bioinformatics community (INSERM).

The aim of this use case will be to explore the possible interactions between already available Galaxy computing services and data repositories, in order to build an integrated and interoperable service for ELIXIR and the wider Life Science user community as a whole(1). The task will build on top of existing national services made available in France and Italy by participating partners, and which are described in the relevant sections of each partner description in section 4. It will aim at fulfilling the following objectives:

· Allow frictionless access to external data sources from different Galaxy deployments

· Facilitate the deployment of Galaxy instances close to the data

· Provide coherency between different existing Galaxy deployments

· Ensure health data security requirements are met throughout the process

In particular subtask T6.6.4 – “Health data security aspects” concerns Legal and ethics requirements on the storage and handling of health data are becoming stricter (e.g. GDPR). In some cases, legal gaps can create obstacles to data sharing and interoperability. This subtask will look at how proposed solutions can be put in place while meeting those strong security requirements.

In the context of the T. 6.6.4 concerning, Health data security aspect, this document aims :

– to define the Legal Framework for the use and re-use of health data for scientific purposes;

– to outline the most important gap deriving from the differences between National laws concerning the processing of health data and the possible solution;

– to suggest a guide for researchers involved in this scenario.

2 Legal Framework

2.1 EU Legal Framework: the principles applicable to health data

Data protection is principle-driven, building on the core principles enshrined in important documents such as Council of Europe Convention 108, the European Union (EU) Charter of Fundamental Rights and the national constitutions of many countries. To ensure full compliance with applicable data protection laws and regulations, natural or legal people who process personal data should adhere to the following data protection principles.

· Fair, lawful and transparent: personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject. In particular, personal data shall not be processed unless permitted by law, based on a preponderant legal interest of the processor or consented to by the data subject.

· **Purpose limitation**: personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

· **Accuracy**: personal data shall be accurate and, where necessary, kept up to date.

· **Data minimization**: personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

· **Storage limitation**: personal data processed for any purposes shall not be kept for longer than is necessary for those purposes.

· **Rights of data subjects**: personal data shall be processed in accordance with the rights of data subjects as stipulated by the applicable data protection laws.

· **Integrity and confidentiality**: appropriate physical, technical, legal and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss, alteration or damage to personal data.

· **International transfer of personal data**: personal data shall not be transferred to a third country or international organization unless that country/organization ensures an adequate level of protection of the rights and freedoms of the data subjects in relation to the processing of personal data.

Regardless of the purpose of processing personal data, such processing is prima facie not permitted unless the data controller has a valid lawful basis to do so (GDPR Article 6). This is enshrined in the first principle of data protection. Six lawful bases for processing are available. No single basis is better or more important than the others – which is most appropriate to use will depend on the purpose of the processing and the relationship with the individual. The lawful basis must be determined prior to the processing, and must be properly documented, as per processing activity. In detail, the six categories are as follows.

· **Consent**: the individual has given clear informed consent for the processing of personal data for a specific purpose.

· **Contract**: the processing is necessary for a contract the data controller has with the individual, or because the data subject has asked steps to be taken before entering into a contract.

· **Legal obligation**: the processing is necessary for compliance with the law (not including contractual obligations).

· **Vital interests**: the processing is necessary to protect someone's life.

· **Public task**: the processing is necessary for the performance of a task in the public interest or as part of an official task or function, and the task or function has a clear basis in law.

· **Legitimate interests**: the processing is necessary for the legitimate interest of a third party, unless there is a good reason to protect the individual's personal data, which overrides legitimate interests; however, this legal basis does not apply if a public authority is processing personal data in order to perform its official tasks.

In the case of data processing activities in the context of health information management tasks, it is obvious that certain types of lawful basis are more likely to apply. Data processing is likely to be carried out based on legal obligation and public tasks; in rare cases, vital interests may apply. Informed consent of the data subject is a critical legal basis: it obviously plays a major role in the case of research activities, but may also have implications for public health purposes that require a high level of completeness of datasets. Consequently, informed consent of the data subject may not be used if there is a basis in the law (such as a cancer registry), or if there is a clear preponderant public interest (as in the case of a pandemic). The concept of informed consent may only be chosen to the extent the data subject has a "real" choice, and if refusal to consent does not have negative implications for the data subject. In practice, informed consent of the data subject is often wrongfully applied, as any legal basis will suffice, and informed consent may have a substantive impact on the outcomes of public health activities. Thus, it is often advisable to select an alternative legal basis, but caution is needed, as transparency requirements continue to apply unless specific exemptions kick in.

2.2 The Regulation in the Italian Law.

In Italy the legal framework concerning the health data is composed by these relevant legislative initiatives:

- D.Lgs 101/2018 which adapts the Code regarding the protection of personal data (Legislative Decree 30 June 2003, n.196) to the provisions of Regulation (EU) 2016/679.
- Deontological rules for processing for statistical or scientific research purposes published pursuant to art. 20, paragraph 4, of the legislative decree 10 August 2018, n. 101 - 19 December 2018 issued by the Italian Data Protection Authority.
- Provision containing the requirements relating to the processing of particular categories of data, pursuant to art. 21, paragraph 1 of Legislative Decree 10 August 2018, n. 101.

The article 7 of Ethics Code regarding sensitive data processed in research activities, establishes that the legal bases include written consent after having read the privacy notice. This is the most important rule defined.

Moreover art. 8 of Ethic Code provides some safeguard measure in order to bridge data protection compliance and ethics rule. In particular the general obligations of compliance with the applicable ethics framework is required. Then healthcare and research purposes shall be distinguished in the privacy information. It is necessary to define an incidental findings policy. Art. 9 of Ethics Code previews that Universities and Research centers shall share awareness and information on the provision introduced in the EC and shall report to data protection authority any violation.

The legal framework introduce some specific rule:

The consent is not necessary:

- When the research in undertaken under a legislative provision, including a research programme established under a specific regulatory framework for clinics art. 12- bis Legislative Degree (Dlgs)30 December 1992, n. 502) and the DPIA is publicly available.
- When, considering specific reasons, to inform data subjects is not possible or it requires an proportioned effort, or it could seriously undermine the research purposes. In these cases, the data controller adopts appropriate safeguards to protect the data subjects' rights and interests, the research has obtained an approval from the competent ethics committee and the Data Protection Authority provided a prior consultation under article 36 GDPR.

Data retention for research purposes could be extended beyond the needed duration in order to pursuing the several scopes that enabled the previous collection and processing according to art. 99 Dlgs 196/2003.

Communication of general data of research staff under art. 100 Dlgs 196/2003 is allowed. Data subjects can in any case exercise their rights.

Privacy notice: art. 105 recalls the general principle of information under article 13 and 14 GDPR unless the effort to inform is unproportionate.

Re-using: The article 110bis of the Italian Privacy Code refers to the re-using of data by third parties. The first condition for it is that data subjects must be informed. Otherwise, a prior authorization from the data protection authority is needed. This approach is not applicable when personal data are collected for healthcare purposes and used for research ones by the same (private or public) scientific hospitalization and care clinics, considering the functional link between the two purposes. The provision seems to refer to patients' personal data before being pseudonymized or anonymized for research purposes, as stated under article 89 GDPR.

Concerning the processing of health and genetic data the provision containing the requirements relating to the processing of particular categories of data requires the following measures:

- The transmission of data in the form of an attachment and not as a text included in the body of the message data encryption taking care to make the cryptographic key known to the recipient through communication channels other than those used for data transmission;
- the use of protected communication channels, taking into account the state of the art of the technology used;
- protection of the attachment in ways suitable to prevent the unlawful or fortuitous acquisition of the transmitted data, such as a password for opening the file made known to the recipient through communication channels other than those used for data transmission.

The use of "web application" communication channels is allowed, which envisage the use of protected transmission channels, taking into account the state of the art of technology, and guarantee, after verification, the digital identity of the server that supplies the service and the client station from which the data is accessed, using digital certificates issued in compliance with the law by a certification authority.

2.3 The Regulation in France Law

The most important legal framework incudes in the France Legal Order:

· DONNÉES MASSIVES ET SANTÉ : Une nouvelle approche des enjeux éthiques - Avis rendu public le 29 mai 2019

· Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties.

On the bases of this legal framework in order to process sensitive data by public research it is necessary the public interests. For genetic data it is necessary the consent of the data subject.

The legal framework require technical and organizational measures for healt data processing for research purposes, in particular:

· Art. 72 establishes that the Ethics Committee must analyze whether or not the data processing meets the public interest;

· Art. 74 introduces the requirement of the Professional confidentiality in processing data;

· Article 73 established that the research shall provide its adherence to the “méthodologie de référence” established by the CNIL, otherwise a specific authorization is required under article 76. The procedure distinguishes the research including human beings from the one that enables personal data flows without involving human beings.

· Monitoring and enforcement activities: the article 77 establishes an audit board “comité d’audit” promoting a system of auditing activities aimed at harmonizing the compliance level of all research activities processing health data.

3 The Application of the EU Regulation: the differences between member state's Legal Order

Although the GDPR harmonises the rules governing the processing of sensitive data, such as personal health data, there are still options for Member States to lay down justifications for processing health data in Member State law. Moreover, Article 9.4 explicitly provides that with regard to processing of genetic, biometric or health data, Member States may maintain or introduce further conditions including limitations. This may mean that in the area of health the GDPR will not be applied in the same manner in each Member State(2). It may also mean that variations in the implementation of the GDPR may arise within one Member State, in particular where regional legislation applies. In addition, the rules under the GDPR applicable to processing of health-related data will be applied in the legal context of the provision of healthcare and the organisation of the health system in a Member State. Such health system specific legal context will set the framework for the implementation of the GDPR and may lead one Member State to lean more towards the use of consent, and another to incline more towards the legal obligation to record all aspects of interaction of a patient with the healthcare system. The national organisation of the health system may also mean that the legal base chosen varies between different categories of care providers, with publicly funded healthcare organisations applying different bases from private healthcare providers, indeed this variation was noted by the correspondent providing information on the application of the GDPR in Spain.

Given that the GDPR foresees the possibility of special legislation for processing of genetic information, it is not surprising that significant variation may exist between some Member States in this area. French and Dutch law provides further examples, since the French law prohibits the automatic processing of genetic data unless express

authorisation is given by the French competent authority (Loi n° 78-17 19783); and the Dutch implementing Act of the GDPR prohibits the processing of genetic data unless that processing 'takes place with respect to the data subject from whom the data concerned have been obtained'. However, both French and Dutch law contain significant exceptions permitting such data to be used for medical purposes: in France, this includes processing by doctors or biologists which is necessary for preventive medicine, diagnosis and care (Loi n° 78-17 1978), while in the Netherlands, the processing of genetic data may also take place for others than the data subject whose data it concerns if a significant medical interest prevails (Article 28, section 2 of the implementing Act (UAVG)). Medical confidentiality will then prescribe that notifying those others will be based on consent of the data subject concerned, though in exceptional cases the genetic counsellor can also fall back on the 'conflict of interests' doctrine in Dutch medical law, in essence stating confidentiality can be waived if that is the only likely way to avoid a life threatening situation of another party.

This potential for fragmentation on the implementation of the GDPR has been noted in the May 2020 Communication from the Commission to the European Parliament and Council entitled "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation" which reviewed two years of implementation of the GDPR in the Member States(3). The report

notes that the GDPR requires Member States to legislate in some areas and provides them with the possibility to further specify the GDPR in others and as a result, a degree of variation has arisen in the implementation of the GDPR which is notably due to the extensive use of facultative specification clauses. The Commission Communication focuses particularly on variations which could create challenges to conducting cross-border business and innovation, in particular as regards new technological developments and cybersecurity solutions. While healthcare is not cited as an example, it is clear that in the context of cross-border care this variation could also add a layer of complexity, and may in turn also create issues for comparability of data in cross-border research. Based on the variations in implementation of the GDPR that can theoretically arise both within and between Member States with respect to processing health related data in the context of Function 1, the first questions of the survey asked national correspondents to clarify which legal bases in Article 6 and 9 are used when health data are processed in the context of care provision. They were asked also to describe their national implementation legislation and give their opinion on implications for care both within their Member State and across borders, both in the case of face to face care provision and eHealth services.

4 Legal Bases for the use of Health data in the context of scientific: the applicability of the OS principles and FAIR Principles

Considering the Legal Framework, it is possible to identify two types of data usage when it comes to “processing of health data for the purpose of scientific research”:

1. Research on personal health data which consists of the use of data directly collected for the purpose of scientific studies (“primary use”);

2. Research on personal health data which consists of the further processing of data initially collected for another purpose (“secondary use”).

In accordance with Article 6(4) GDPR, data can only be further processed for a purpose other than the purpose stated at the time of collection if it is compatible with that purpose (known as the purpose limitation principle). When it comes to research however, this should be read in conjunction with Article 5(1)(b) which carves out a privileged position for research, stating that further processing for scientific research purposes in accordance with Article 89(1) is not considered incompatible with the principle purpose. However, it should be borne in mind that the EDPS, building on recital 159 of the GDPR, makes a distinction between ‘genuine research’ and other research in this respect (EDPS 2020). That distinction is important. Research should meet methodological requirements, standards of research integrity (KNAW 2018), and aim to contribute to the common good. Given the respondents and the regulations which are referred to in this chapter, the research discussed here falls into that category of genuine research.

The GDPR permits processing of health data for research purposes where one of the lawful bases set out in Article 6.1 applies and the data controller can also meet one of the relevant derogations in Article 9.2, otherwise the processing of special categories of data such as health and genetic data is prohibited

The GDPR provides that Member State legislators may adopt legislation to allow for use of data for research in accordance with Article 9. 2 lett. j and 89.1. It is clear from the responses provided by the correspondents that the Member States have not implemented such legislation in a homogenous way, resulting in a complex and fragmented landscape for researchers to navigate. Consequently, differences between Member States in the way the GDPR is implemented and interpreted in the area of scientific research has made data exchange between Member State and EU bodies for research purposes difficult and in some cases highly technical. Variation also exists between Member States in how they distinguish between public and non-public sector researchers. This is relevant as the definition can influence the selection of lawful basis. As pointed out by participants in the workshops, the distinction between public and non-public research is not always clear-cut, and many hybrid forms exist, notably when commercial organisations provide unrestricted grants for research conducted in public universities.

This is relevant because in addition to relying on the provision for scientific research in Article 9.2 lett. j certain categories of researchers may also be able to rely on Article 9.2, lett. i where research is in the public interest. This will however be difficult for researchers in for-profit organisations who may find it challenging to prove that research is in the public interest. The public interest legal basis can only be invoked where such processing is provided for in Member State or EU law. This will demand that the legislator defines which type of researchers may make use of the public interest criterion. It will also demand that the legislator has weighted the risks to the individual against public benefits. One such balance test applied in the context of research has been called the 'duty of easy rescue' test(4) . The 'duty of easy rescue' may be described as arising when it is possible to benefit others at no or minimal cost to oneself. Porsdam Mann et al argue that where the duty of easy rescue does not apply because there are significant risks involved in data sharing and where these risks cannot be minimized by security management, research can only ethically proceed without informed consent when obtaining consent would be impossible or impracticable, the public benefit of the research very significantly outweighs the risks, the public is adequately informed, and any resulting harms are compensated. These balances as described have however not yet been developed into easily applicable criteria in national or EU level law which adds further complexities(5). This study seeks to examine and analyse the legal patchwork and technical burdens which have emerged across Member States in particular looking at Article 89.1 safeguards for research and lawful bases as provided for in the GDPR.

5 Pseudonymisation and anonymisation

The GDPR compliance constitutes a logical priority to enable research data towards a FAIR ecosystem(6). Therefore, the standardization of procedures and requirements to allow the openness purposes may facilitate the achievement either of GDPR compliance purposes or Open Data ones. Combining technical safeguards with practical requirements and standards could facilitate the standardization of some recurrent processes, required for re-using data, like pseudonymization procedures. For example, Belgian law establishes, in the case of health data processed for research purposes, that pseudonymization could not be performed by the data controller, but by an independent body, who is subject to specific confidentiality obligations (i.e., professional secrecy). The “technical separation” between those who perform the two activities and an explicit obligation for those who pseudonymize to avoid re-identification might constitute a barrier in the case of cross-border partnerships. To harmonize best practices on the fundamental conditions to process personal datasets for research purposes would facilitate also the interoperability and re-use of research data.

6 Harmonization of Safeguards for Selected Sectors (e.g. Health, Genetics)

Each Member State may decide to adopt general safeguards for personal data processed for research and statistics purposes, but it could also decide to regulate several profiles of a specific sector, including the related data management. Safeguards may at least be standardized under the parameter of data subjects' categories/vulnerabilities, whose fundamental rights shall be enhanced as a priority of Open Science policies. Adopting similar measures for homogenous categories of data, considering the plurality of grounds of vulnerabilities stated under Articles 9 and 10 GDPR, would Facilitate the identification of common technical bases to make research data interoperable and re-usable beyond the specific means applied for data processing(7).

Article 9.2 lett. j GDPR requires that Member State or EU law which provides for the processing of sensitive data for scientific research purposes in accordance with Article 89.1 shall include the use of suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Article 89.1 holds that safeguards shall ensure technical and organisational measures are in place to uphold the principle of data minimisation and goes on to highlight some measures which may be used to achieve this principle such as pseudonymisation or anonymisation(8).

7 Best Practices for the implementation of Scenario 3

In the phase of implementation of the research activities concerning Scenario 3, Researchers must take into account some accommodation considering data protection and security measures processing health data(9).

In the implementation of Scenario it has been necessary to consider this milestone in order to apply GDPR and Nationals Law applicable in processing data(10):

- If in the process there are any information that identifies (directly or indirectly) a human person:
  - To cooperate with the DPO or the ethics advisor or the ethical-legal unit of the organization or Universities in order to provide the compliance actives.
- In in the process there are special categories of data.
  - To implement the technical and organizational measures require (on the base of the legal framework identified) to protect data lows in terms Availability, Confidentiality, Integrity.
  - In in is necessary to consider:
    - To comply of the processing under article 30 GDPR;
    - To define impact evaluation under article 35 GDPR;
    - To regulate the governance under articles 26 and/or 28 GDPR if third parties are involved in the processing (so-called external governance);
    - To inform data subjects;
    - To obtain the approbation of the competent ethical committee (if required);
    - To perform training activities for collaborators, instructed and therefore authorized them under article 29 GDPR (so-called internal governance);
    - To obtain a commitment for confidential obligations (if required);
    - To introduce procedures to ensure data subjects to exercise their rights;
    - To introduce regulation and procedures for data breach;
    - To define proper technique of pseudonymization;
    - To identify how to encrypt your data;
    - To plan stress tests to identify infrastructural vulnerabilities;
    - To plan planned auditing activities.

- Check the data retention limit and verify if you have anonymized data or deleted them accordingly or plan the necessary actions.
- Determine how long you shall store informed consent from research subjects and act accordingly.
- Remove any access to no longer authorized entity/bodies/collaborators shall be removed.
- Check if you have pursued all the instructions you provided within the data management plan.
- Re-use policy shall be clearly identified.

- Proper retention location and access privileges for data whose further use is enabled should be identified and consequent actions adopted(11).

8 References

No	Description/Link
1	M. A. TANGARO, G. DONVITO, M. ANTONACCI, M. CHIARA, P. MANDREOLI, G. PESOLE, F. ZAMBELLI, Laniakea: an open solution to provide Galaxy “on-demand” instances over heterogeneous cloud infrastructures, in GigaScience, Volume 9, Issue 4, April 2020, https://doi.org/10.1093/gigascience/giaa033
2	European Commision, Assessment of the EU Member States’ rules on health data in the light of GDPR, Luxembourg, 2021, available to this URL: https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf
3	Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM(2020) 264 final, available to this URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264
4	S. PORSDAM MANN, Y. DONDERS, C. MITCHELL, V. J. BRADLEY, M. F. CHOU, M. MANN, G. CHURCH, AND H. PORSDAM, Advocating For Science Progress As A Human Right, in PNAS, 2018, Vol. 115, n. 43, https://doi.org/10.1073/pnas.1816320115
5	M. BLOCH; O. GÜNLÜ; A. YENER; F. OGGIER; H. V. POOR; L. SANKAR; R. F. SCHAEFER, An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications, in IEEE Journal on Selected Areas in Information Theory, Volume 2, Issue: 1, March 2021, pp. 5-22, 10.1109/JSAIT.2021.3062755
6	F. ZUIDERVEEN BORGESIUS, J. GRAY E M. VAN EECHOUD, Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework, in Berkeley Technology Law Journal, Volume 30, n. 3, 2015, pp. 2073-2131, https://www.jstor.org/stable/26377585 ; Y. MCDERMOTT, Conceptualising the right to data protection in an era of Big Data, in Big Data & Society,June 2017. doi:10.1177/2053951716686994
7	European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
8	A.COHEN, K. NISSIN, Towards formalizing the GDPR’s notion of singling out,, in Proceedings of the National Academy of Science of The United States of America, 2020, 117, (15), pp. 8344-8352, , 10.1073/pnas.1914598117
9	Organisation for Economic Co-operation and Development (OECD), Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data adopted on 23 September 1980 and Amended on 11 July 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 Report on the implementation of the recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, C(2021)42, 17 March 2021. https://one.oecd.org/document/C(2021)42/en/pdf
10	N. FOGGETTI, M. GERIN LASLIER, MARYVONNE; S. DI GIORGIO, N. HAILE GEBREYESUS, S. MÜLLER, I. VAN NIEUWERBURGH, G. ROMIER, J. VAN

	WEZEL, L. HÖNEGGER, A. BODLOS, M.VERNET, Legal and Policy Framework and Federation Blueprint, D4.6 Eosc-Pillar, 2021, 10.5281/zenodo.5647948
11	D. MARK, D. WILKINSON, M. DUMONTIER, B. MONS, The FAIR Guiding Principles for scientific data management and stewardship, in Science, 2016. https://www.nature.com/articles/sdata201618