EJP RD
European Joint Programme on Rare Diseases

H2020-SC1-2018-Single-Stage-RTD
SC1-BHC-04-2018
Rare Disease European Joint Programme Cofund

Grant agreement number 825575

Requirements for GDPR Implementation in Pillar 2

From EJP RD Deliverable 10.1 "First Annual strategic report and Action plan for Pillar 2, including: Systematic surveys reports, QMS of Pillar 2 description, GDPR compliance report and sustainability planning reporting"

Table of contents

1. Requirements for GDPR Implementation in Pillar 2

General Data Protection Regulation (GDPR) has become the main regulatory framework for general-purpose data protection on the European level in 2016, with national implementations following. The GDPR is, however, not the only regulation: specific domains have their own additional regulatory frameworks, such as clinical trials.

These recommendations follow FAIR[1] and FAIR-Health[2] principles in order to maximize the value of the data for research purposes. These are initial requirements that will be further elaborated upon into more technically detailed measures during the course of development of the EJP RD Virtual Platform (VP).

1.1. Definition of roles and data

- For each legal entity involved in processing of the data subject to data protection, their role MUST be defined (data controller, data processor).
- For each data made accessible via VP of EJP RD, it MUST be clear which legal entity is data controller and it MUST be specified what is legal basis for processing the data. Definition of the data controller and contact information for that data controller must be kept as a part of metadata accompanying the data.
- Data controllers MUST inform data subjects about the extent of the processing of personal data and how data subjects can execute their rights.
- Data controllers MUST collect and archive provenance information about data collection process.

[1] Wilkinson MD, Dumontier M, Aalbersberg IJ, Appleton G, Axton M, Baak A, Blomberg N, Boiten JW, da Silva Santos LB, Bourne PE, Bouwman J. The FAIR Guiding Principles for scientific data management and stewardship. Scientific data. 2016;3.
[2] Holub P, Kohlmayer F, Prasser F, Mayrhofer MT, Schlünder I, Martin GM, Casati S, Koumakis L, Wutte A, Kozera Ł, Strapagiel D. Enhancing reuse of data and biological material in medical research: From FAIR to FAIR-health. Biopreservation and biobanking. 2018 Apr 1;16(2):97-105.

- EJP RD VP SHALL provide a registry of those data sources that are part of the VP and monitor compliance with the requirements.

1.2. Processing personal data

- Privacy enhancing technologies SHOULD be used when processing personal data to protect privacy of data subjects (unless there is justification why it cannot be used). Selection of privacy enhancing technologies MUST be assessed to balance ration between acceptable residual risk and maximizing utility and reliability of the data. Documentation of that assessment process MUST be kept.
- Recipient of the data MUST be informed about any consequences of application of the privacy enhancing technologies that might impact meaningfulness, reliability or reproducibility of the anticipated research.
- When data is released for a particular purpose, extent of the data MUST be minimized to the set necessary to achieve that purpose.

1.3. Execution of data subject rights

- Provenance information MUST be kept about data releases for research purposes. This is necessary to allow effective implementation of data subject rights.
- For each data set a contact point MUST be defined to allow data subjects to execute their rights.

Overview of processes related to data is available in a guideline[3], including when exemption for research applies based on GDPR Art 89.

1.4. Anonymization and processing anonymous data

Anonymization is a process of rendering data non-personal and hence the resulting data being outside of protection domain. Anonymization is, however, inherently imperfect process balancing between utility of the resulting data and residual risk of reidentification[4,5]. For this reason, the following requirements and recommendations should be taken into considerations by the VP of EJP RD:

- Anonymization process is processing of personal data and as such the controller MUST have documented legal basis for anonymization.

[3] Page 104 of Radim Polčák, Leoš Ševčík, Michal Koščík, Jakub Klodwig, Petr Holub. Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR. Zenodo; 2018. doi:10.5281/zenodo.2533865.
[4] Section 1.1 of Dwork, C and Roth, A. The algorithmic foundations of differential privacy. Theoretical Computer Science 2013;9:211– 407.
[5] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., & Ristenpart, T. (2014). Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing. Proceedings of the USENIX Security Symposium. UNIX Security Symposium, 2014, 17–32. Retrieved from http://www.biostat.wisc.edu/page/WarfarinUsenix2014.pdf

- When possible, anonymized data should be avoided for medical research because of hard to assess impact of anonymization on data quality.
- When aggregating data sets, the anonymization shall be implemented after aggregation in order to minimize harm done to the data[6], unless there is some other restriction preventing aggregation of non-anonymized data (e.g., missing legal basis for aggregation).
- Anonymized data shall be regarded as having non-zero risk of reidentification and therefore the recipient of the data must agree with not attempting to reidentify persons from the anonymized data set. This also applies transitively to any further data recipients that receive the data from the first recipient.

1.5. Compliance of infrastructure

The infrastructure operators for the VP are advised to adopt relevant certifications such as FitSM[7], ISO 27001, possibly combined with ISO 27017 and ISO 27018, or at least build the infrastructure with according to the requirements for those certifications. This is in order to help demonstrating their compliance when operating the infrastructure for processing personal data.

[6] PR-5 rule of FAIR-Health: Holub P, Kohlmayer F, Prasser F, Mayrhofer MT, Schlünder I, Martin GM, Casati S, Koumakis L, Wutte A, Kozera Ł, Strapagiel D. Enhancing reuse of data and biological material in medical research: From FAIR to FAIR-health. Biopreservation and biobanking. 2018 Apr 1;16(2):97-105.
[7] https://fitsm.itemo.org/