GDPR FAQ for BESTPRAC

Based on BESTPRAC Members' Experience

BESTPRAC WORKING GROUP LEGAL (WG3)
WG3 Vice-leader: Niina Mikkonen, Aalto University, Finland

2019

This GDPR FAQ document is aimed at assisting administrative, financial and legal staff at universities and research-driven institutions, in particular TN 1302: BESTPRAC participants. Aim is to provide help with the GDPR related questions that arise during the research projects. This document is provided for information purposes only and its content is not intended to replace consultation of any applicable legal sources or the necessary advice of a legal expert, when appropriate. Neither the author(s) of this document or any BESTPRAC WG Legal or other WG members contributing to the preparation of this document by sharing their knowledge, experience or best practices while discussing GDPR issues during WG3 meetings or ex-post can be held responsible for the use made of this document. The author(s) would like to acknowledge the contribution and networking support of the COST Action TN1302.

Regulation (EU) 2016/679 of the European Parliament and of the Council, the European Union's General Data Protection Regulation ("GDPR"), regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

1. In a collaborative research project – who are independent data controllers for research data? Who are joint controllers for research data?

- According to GDPR the **data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- If universities are determining the use of data e.g. with the funders, usually universities are controllers for research data – not the individual researchers
- If the use of data is planned together (the universities together decide the purposes and means of data use), universities are joint controllers
- If each university makes their own research management plans, they are independent data controllers
- An annex to the consortium agreement (or a separate agreement) should include a flow chart of the data between the partners and the terms concerning the processing and use of personal data

2. Which 'lawful basis' can be invoked for processing personal data for research purposes by a university?

- Article 6 of GDPR defines the lawful basis for processing personal data
- Performance of a task carried out in the **public interest** (art. 6.1. e) – must be defined in national law. E.g. an EU or a nationally funded project is usually scientific research and therefore a task carried by public interest
- Informed and specific **consent** given by the data subject (art. 6.1. a)
- If research is carried out by company, also **legitimate interest** (6.1. f) can be used
- Using public interest as lawful basis allows wider possibilities for use of research data

3. Which lawful basis can be invoked for processing special categories of data?

- Special categories of data means racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
- Article 9 of GDPR defines the lawful basis for processing special categories of data
- For research purposes you can consider applying explicit consent (art. 9.2. a) or scientific research (art. 9.2. j)

4. What about personal data received from children for research purposes? Do universities need a parental consent?

- Main rule/principal rule: Use the "the public interest" as a legal bases for processing
- If "the public interest" is not an option, use the consent as the legal basis for processing
- However, when using consent as legal basis consider whether the individual child has the competence to understand and give consent for themselves – if not, the child's consent will not be valid

- Where a child is not competent to give consent, the consent of someone with parental authority over them should be obtained
- In principle, GDPR gives children and adults the same rights over their personal data. If children are competent to exercise their rights under applicable national law, no parental consent is needed. Some jurisdictions set a minimum age for competence, while others rely on examination of the child's development. Therefore, universities should only request parental consent if one of the following conditions apply:
    - The child authorizes his or her parents to exercise these rights on his or her behalf
    - The child doesn't have sufficient understanding to exercise the rights himself or herself
    - There is convincing evidence that parental consent is the child's best interest
- Check also national ethical guidelines

5. What to do when somebody withdraws its informed and specific consent? How does withdrawal affect the research?

- No further processing is allowed if a data subject withdraws his or her consent (art. 7.3)
- The controller is required to delete or anonymize the personal data if it wishes to continue using the data
- However, the controller may retain the personal data to comply with legal obligations or for scientific research purposes if deletion would be likely to render impossible or seriously impair the achievement of the objectives of such processing (art. 17.3)
- Use prior to withdrawal remains legal

6. In what cases university should use model contractual clauses for transferring data outside of EU?

- EU model contractual clauses should be used whenever data is transferred to a country outside of the EU that doesn't offer an adequate level of protection, as confirmed by an adequacy decision of the EU Commission (art. 45)
- Check if the country has received adequacy decision from EU commission – no need to use model clauses
- List of countries with adequacy desicion
- Privacy shield certification is available for US organizations – Check if the US organization has privacy shield certification – no need to use model clauses (so far US universities have not pursued privacy shield certification)

7. When university needs a Data Processing Agreement?

- Data Protection Agreement (DPA) is a written contract between the organization processing personal data (data processor) on behalf of another organization
- According to GDPR the **data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (see the explanation for **data controller** in the question number 1)
- DPA is necessary if university contracts third parties for purposes defined by universities for processing of personal data, e.g. for transcribing of interviews
- Please also consider answers to the questions number 6 and 9

8. What is the difference between anonymized data and pseudonymised data?

- **Anonymization** refers to the process of removing personal identifiers (direct or indirect) that may lead to an individual being identified from that information, or combined together with other information
- If it is possible to completely anonymise your data (meaning that there is no key to trace back to the individual person, it is not considered personal data and is thus not protected by data protection regulations
- If the data cannot be completely anonymised for whatever reason, data protection regulations applies
- Anonymization is quite hard to achieve, see "WP 29 opinion 05/2014 for anonymization techniques: https://www.dataprotection.ro/servlet/ViewDocument?id=1085
- **Pseudonymisation** refers to replacing the possibility to identify personal data by pseudonym (art. 4.5)
- If the code that would link the data to real identities is preserved, the data is not anonymized but only pseudonymised
- Personal data which has been pseudonymised is protected by data protection regulations

9. What is the territorial scope of GDPR? Do non-EU based organizations need to comply with the GDPR?

- Art. 3 determines the territorial scope
- The regulation applies to the processing of personal data
    - (1) in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not;
    - (2) data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
        - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
        - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union;
    - (3) by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law
- In other words, all organizations based in the EU have to comply with GDPR. This is also valid for:
    - non-EU based organizations if they process EU citizens personal data in the EU or elsewhere;
    - in any cases in which EU-citizen or non-EU citizen personal data are processed within the territory of the EU.
- E.g. if research data collected from data subject in the EU is transferred to non-EU based organizations; or those organizations collect the data from EU-based data subjects, the organizations need to comply with GDPR
- Please also consider answer to the question number 6

10. Does the GDPR provide exceptions for academic research? What kind of exceptions?

- Art. 17.3. d: There is an exception to the right to be forgotten for scientific research
- Art. 89: Where personal data is processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Art. 15 (Right of access by the data subject), 16 (Right to rectification), 18 (Right to restriction of processing) and 21 (Right to object).

- Art 13: There is an exception to information to be provided where personal data is collected from the data subject – it is not necessary to impose 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. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

11. Where and how personal data collected for research purposes should be stored or should not be stored?

- Art. 5.1. e: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes
- Research data can be stored as long as it is needed to validate research findings and results
- Key element is the data security: consult your university IT services and follow their instructions in order to ensure data security
- It is not advised to use memory sticks
- Do no use email for research data containing personal data
- Consider using only centrally encrypted laptops
- In case of physical storage: locked storage with no access by other persons

12. What can be considered as a personal data breach in research and what to do when it happens?

- E.g. loss of memory stick containing personal data collected in the research
- If your research data is subject to a personal data breach, you need to consider whether this poses a risk to people. If there is a risk, contact your university Data Protection Officer (DPO).
- You and DPO need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach
- If it is likely that there will be a risk then the DPO must notify the supervisory authority within 72 hours. If it is unlikely then there is no need to report.
- If there is a high risk, also affected individuals need to be informed about the breach without undue delay. When contacting affected individuals you need to tell them what data has been compromised and how they can protect themselves from negative effects. Consider providing help for affected individuals.