FGB Policy Positions on the GDPR

2022-09-19; Version 2.1

The European General Data Protection Regulation (GDPR) specifies how personal data must be managed and protected by organizations located in Europe. Almost all data used by FGB researchers are about human beings and the majority of this data qualifies as personal under GDPR definitions. The GDPR addresses many issues, but leaves a lot of details up to interpretation. This document sets out how FGB interprets and implements GDPR requirements for research in the faculty. Additional detail about what the GDPR is and what it means for FGB researchers can be found in this short summary.

1. Directly identifying personal data (e.g. name, address, contact information) may be maintained for the entire duration of a research project if this information is required to carry out the project. For example, it may be necessary to: contact individuals about the next phase of the project; contact participants for a follow-up project, if they have given consent to be contacted for that reason; or for communication with participants' caregivers or teachers who may need to provide supplementary information about participants, but who should not know the identification code under which participants are registered by the research team. Directly identifying personal data should be stored separately from other research data, at a higher level of security than indirectly identifying information and they should only be accessible to those individuals (usually research assistants and data managers) who absolutely require access to them and only for the period for which access is required (i.e. once access is no longer required, access rights should be revoked).
    a. If it is not feasible to store directly identifying data in a separate storage location from all other research data, these data should be stored in a separate folder with controlled access rights to only those who need to know these data and ideally with encryption on the folder or the file itself that contains the data.
    b. If it is not feasible to separate directly identifying data from the research data which need to be analyzed (e.g. photographs or audiovisual data), the storage solution used for the data should provide the highest possible level of security and/or encryption should be used.
    c. Information on how to archive directly identifying personal data can be found in the local FGB implementation of the DSW National Guidelines on Archiving.

NB: The Security Tips on De-identification and on Secure Storage provide additional guidance on how to handle directly identifying data.

2. The fundamental legal basis for conducting a research project using personal data should, in the majority of cases, be the informed and freely given consent of participants. Legitimate interests can in some specific cases be invoked as an alternative legal basis for conducting a research project if obtaining informed and freely given consent is impossible or would impair

the aims of said project. In order to use legitimate interests as a legal ground for conducting a research project, the benefits of the research project must outweigh the rights of the individuals whose data are being used. Additional conditions are also required if special categories of personal data will be processed on the basis of legitimate interests (see Rule 5 from Privacy in Scientific Research – 10 Key Rules). Situations where legitimate interests may be more appropriate than obtaining consent include, but are not limited to: a. Child abuse (cannot ethically inform the parents, but the child is <16 years old) b. Youth crime (cannot ethically inform the parents, but the child is <16 years old) c. Misconduct in public organizations/the church/social support (cannot inform the individuals responsible for misconduct without risking harm to others or to the aims of the research project) d. Historical research where it is no longer possible to contact the subjects

This is not an exhaustive list; there may be many other cases where legitimate interests could be an appropriate legal ground for conducting a research project. However, applying this legal basis requires additional effort from the researcher to ensure that the privacy of the individuals represented in the data is sufficiently protected. Researchers wishing to invoke legitimate interests as a legal basis for their research project must:

a. Seek advice from the FGB privacy champion (research.data.fgb@vu.nl) as to whether invoking legitimate interests is feasible

NB: The privacy champion will discuss the case with the privacy lawyers for Legal and Institutional affairs; the FGB Scientific and Ethical Review Committee (VCWE) and FGB data protection officer may also participate in these discussions.

b. Complete a Legitimate Interests Assessment and a Data Protection Impact Assessment.

NB: Legitimate interests CANNOT be used as grounds to conduct clinical research that falls under the purview of the Good Clinical Practice Guidelines and/or the WMO; informed and explicit consent is a requirement for these types of research, except in the extreme case of emergencies (WMO Article 6.4 and ICH-GCP E6/R2 Addendum 4.8.15).

3. FGB is working to meet the FAIR-principles and data sharing goals. However, almost all of the data utilized at FGB is about human subjects and the vast majority of this data cannot be sufficiently anonymized to both meet current definitions for anonymity and remain useful for reuse. This means that when data are collected at FGB, researchers should ensure that informed consent is also obtained from participants for the reuse of the data, regardless of whether the data will be reused by the original research team or by new researchers at other institutions in the future. It should be clear to the subject reading the consent form whether they are giving consent to the former, the latter or both.

NB: It is insufficient to simply ask: “Do you consent to the reuse of your data for new research?”, as this is not sufficiently informative. For support on how to obtain consent for the reuse of research data that cannot be sufficiently anonymized see this checklist and contact the FGB privacy champion if there are additional questions.

For research projects that have already started, but for which consent was not obtained for the reuse of data, researchers should contact the FGB privacy champion for advice on how to proceed with regards to data reuse and sharing.

4. FGB researchers are encouraged to utilize existing sources of research data, for example, data found in research data repositories. Despite these data being available for reuse, it is still the responsibility of FGB researchers to: a. Determine whether the data could be considered personal data under the GDPR and whether it is legal for the data to be reused; b. Determine whether the research subjects in the data could be informed about the reuse of these data, if appropriate.

Oftentimes, excessive effort would be required to determine who the research subjects are and what their current contact information is. If the FGB researcher has determined that they are allowed to reuse the data, but directly contacting subjects with details about the new research is impossible, then a form of passively informing subjects about the new research is advised. An information letter containing the requirements described in Article 14 of the GDPR and further explained in this checklist should be made publicly available, for example on a study website. FGB researchers can contact the FGB privacy champion for additional support on this topic.

5. A research project is exempt from the GDPR's right to be forgotten if data erasure "renders impossible or seriously impairs the achievement of the objectives" of the project. If a study participant wishes to exercise this right, but the project is already in the analysis phase or later, researchers may refuse this right: once data have been analysed, published and/or archived, the data can no longer be deleted without severely impairing the aims of research. Regardless, requests for the right to be forgotten must always be forwarded to the VU Data Protection Officer (functionarisgegevensbescherming@vu.nl), who will lead the communications between the requesting participant and the researchers. a. If a participant revokes consent to a research project, the usage of the data already collected depends on the nature of the research project and the phase of the research cycle. If a research project consists of repeated measurements and a participant revokes consent by saying that they no longer wish to be contacted or to take part in the study, all of the data collected up until that point may still be used, unless the individual exercises the right to be forgotten and the erasure of the data is not detrimental to the aims of the research project. If a participant revokes consent to the entirety of the research project, without invoking the right to be forgotten, and the research project is still in the data collection phase, the data do not need to be deleted, but they may not be used for analysis; if the research project is in the analysis phase or later when the participant revokes consent to the entirety of the research project, the data cannot be deleted; these data however should be flagged as not to be used for any follow-up research projects.

6. Any requests from a research participant for the GDPR's right to data portability[1] will be reviewed on a case-by-case basis with the VU Data Protection Officer

[1] There are limitations to the right to data portability. It can only be exercised if the legal basis for processing was consent or for the performance of a contract, and only if the data are digital. The data must have been directly obtained from the subject and not further

(functionarisgegevensbescherming@vu.nl). Such requests are not expected to occur very often, and as such, FGB researchers are NOT required to prepare for any such requests (i.e. by ensuring that the data in question are machine-readable). FGB researchers are not obliged to execute requests for data portability if this would risk the privacy of other individuals or severely harm the aims of the research project, but, ultimately, the decision to approve a request for data portability lies with the Data Protection Officer for the VU.

7. Long-term research projects should occasionally update consent. This should be done if there are any fundamental changes to the nature of the study, such as a change to the purpose of the study, the types of data collected, or any planned data sharing that was not mentioned earlier. FGB researchers should also review their consent forms every ten years to determine if consent needs to be refreshed. a. Consent forms from long-term research projects that started prior to the implementation of the GDPR should be reviewed for compliance with the GDPR. If found to be non-compliant, researchers must attempt to refresh participant consent. If it is not possible to obtain refreshed consent from all participants, for example, due to changes in contact information, data may continue to be used based on the original consent; however, an updated information letter about the changes to consent and participant rights should be made public, such as on a study website, so that the individuals who could not be contacted can find such information and can contact the researchers for more information, if necessary. FGB researchers can contact the FGB privacy champion for advice on what to include in this information letter.

8. FGB researchers are expected to assess whether a Data Protection Impact Assessment (DPIA)[2] must be completed and to complete the DPIA to the best of their abilities. The FGB privacy champion will provide initial advice on DPIAs and if complex issues are identified, the privacy champion will forward the DPIA to the privacy lawyers for VU Legal and Institutional Affairs for additional support. a. DPIAs should be occasionally refreshed for long-term research projects. For cohort studies with discreet collection phases, DPIAs should be reviewed and updated prior to each new collection phase if at least 5 years have elapsed since the last collection phase. Long-term registries (e.g. NTR, NAR) that are continuously collecting data should conduct a new DPIA at least every 5 to 10 years. Any research project that previously required a DPIA must complete a new DPIA if there are fundamental changes to the project, such as new purposes, new methods of data collection or new technologies being utilized for data collection and analysis.

---

manipulated (therefore a calculated depression score would not apply, whereas an unaltered MRI would). The data provided must be in a machine-readable format, such as XML, JSON etc. The FGB research data officer and TO3 can assist in making machine-readable documents.

[2] FGB Researchers can fill in a pre-DPIA questionnaire to determine if a DPIA is *legally* required. Even if a DPIA is not legally required, it is still recommended to conduct one to ensure that all GDPR requirements are met.

9. Non-digital personal data (such as saliva samples or written documents) must be protected from theft, loss, damage and unauthorized access, just like any other personal data. Safe transport of non-digital data is described in the FGB Security Tips on Physical Transport.