GDPR for Researchers

General Data Protection Regulation

Stevner, Lene; Sandøe, Peter

Publication date:
2018

Document version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Stevner, L., & Sandøe, P. (2018). *GDPR for Researchers: General Data Protection Regulation*. Department of Food and Resource Economics, University of Copenhagen.

UNIVERSITY OF COPENHAGEN
FACULTY OF SCIENCE
DEPARTMENT OF FOOD AND RESOURCE ECONOMICS

GDPR for Researchers

General Data Protection Regulation.

Authors: Data Quality Coordinator Lene Stevner, NEXS, SCIENCE,
and Professor Peter Sandøe, IFRO, SCIENCE, and IVH, SUND/
Sept. 2018, version 1.10

What is GDPR?

GDPR regulates the processing of personal data relating to individuals when data are processed in an EU Member State.

The purpose of GDPR is to impose a uniform level of privacy protection within all Member States when data are processed in the Member State or transferred to other Member States within the EU/EEA.

This puts companies, researchers and other actors on a level playing field when it comes to personal data protection. Due to the EU's global importance in trade and international science, GDPR will have an impact on personal data protection requirements globally.

The privacy and data protection requirements of GDPR include:

- Consent of subjects to data processing
- The need to anonymise collected data as soon as possible to protect privacy
- Provision of personal data breach notifications to authorities
- Requirements for safe handling and transfer of personal data across borders
- The need for larger companies and institutions to appoint a data protection officer (DPO) to oversee GDPR compliance (University of Copenhagen (UCPH) has appointed Lisa Ibenfeldt Schultz as DPO).

LINKS

- DPO: lis@adm.ku.dk
- Legislative acts
- KU-guide in Management of Personal Data – Research Portal

Which data count as personal?

Any information which can directly or indirectly be linked to an identifiable person counts as personal. This definition means that a wide range of data are personal, including names, identification numbers, location data or online identifiers.

Personal data in research?

The processing of personal data in research projects must comply with the GDPR.

Why?

Apart from the need to comply with the legislation, additional requirements are imposed by funders, journals and the institutions to which international collaborators belong.

Potentially there are grave economic consequences: The University of Copenhagen (UCPH) can be fined up to four per cent of annual global turnover for breaching GDPR, or 20 million euro.

What must a researcher do to comply with GDPR?

Before the project

All projects involving the collection, handling and/or processing of personal data must be registered at the University by completing the registration form (see link below).

If personal data are entrusted to external processors who are to perform a task or handle the data for the University, a data processing agreement must be concluded and signed by the Head of Department. A copy must be sent to the Faculty Secretariat. The Tech Trans Office negotiates the data processing agreement if the main contract is negotiated by them.

For data processors outside the EU, the Standard Contractual Clauses Template must be used as the agreement with data processors and signed by the Head of Department. A copy must be sent to the Faculty Secretariat. The Tech Trans Office negotiates the agreement if the main contract is negotiated by them.

Project managers who grant students access to research data must enter into a data processing agreement with the individual student. A model contract form is under preparation.

Create a project-ID list. The ID list must be the only document/key connecting the subject's personal data/biological samples with his or her name or other identifiers. It must restrict access to the identity of the subject via a unique project-ID. Store the project-ID list separately from all other documents or biological samples.

All study documents and samples must be identified only by project-ID (pseudonymised).

The ID list in hard copy must be stored under lock and key in a "room" with a limited number of keys and restricted access.

The electronic ID list must be stored in a folder on the H-drive or the S-drive if it is to be shared with other staff.

"One Drive Business" can be used for sharing with external collaborators, but all personal data must be encrypted.

Implement a "Good Data Management Procedure" for handling personal data.

Train project staff in the procedures.

The project manager is responsible for carrying out an impact assessment if personal data are to be processed in research projects and the processing of personal data will result in a high risk to project participants. The impact assessment must be sent to the Faculty Secretariat after approval by the DPO.

NOTE that there may be requirements going beyond those relating to the processing of personal data:

If the trial includes biological material and/or a medicinal product or a medical device, additional approvals from a committee on health research ethics and/or the Danish Medicine Agency is mandatory.

For other research it may be advisable to apply for permission at the Research Ethics Committee for SUND and SCIENCE.

During the project

Data subjects must give informed consent to the processing of their personal data for one or more specific purpose or protocol.

The researcher must be able to demonstrate that the data subject has consented to the processing of his or her personal data: Archive the Informed Consent Forms or other documentation under lock and key or on the S-drive as a scanned copy.

New data processing agreements must be completed in an ongoing way when new processors become involved and always before data are transferred to the processor.

ID lists are to be updated in an ongoing way as long as subjects are included in the project and their data are recorded.

LINKS

- Registration form
- Processing of sensitive data in health and social sector
- Privacy impact assessment
- Agreement with data processors
- Standard contractual clauses
- Student Contract (under preparation)
- Create a folder on S-drive
- Guidelines about notification etc. of a biomedical research project to the committee system on biomedical research ethics (in Danish)
- Research Ethics Committee for SCIENCE and SUND
- Guideline for applications for authorisation of clinical trials of medicinal products in humans
- Application for clinical investigations for medical devices

The project should be considered as ongoing for as long as the data are being processed.

Where personal data are no longer required for the project, they must be anonymised – the sooner the better.

Data are anonymous when it is no longer possible for anyone (including the researcher) to re-establish

the identity of the subject with reference to remaining information/data. Hence proper anonymisation requires the ID list to be destroyed. Qualitative data may need to be checked and redacted to remove information that could serve to identify a specific person.

Likewise, with biological material it may be necessary to delete or remove certain meta-data.

After the project

A project can only be viewed as ended when anonymisation has been successfully completed or, as the only alternative, transferred to the Danish National Archives (Rigsarkivet).

Good Clinical Practice (GCP) Guidelines require the archiving of source data for 15 years. (A new EU regulation expected to apply from 2019 will extend that period to 25 years.)

The Danish government's "patient insurance" requires material to be archived for 10 years.

The Ethics Committee Act requires that sources are stored for as long as clinical analyses are being performed and clinical findings can be made. It also requires the subject to be informed.

Non-anonymised data can only be archived at the Danish National Archives (Rigsarkivet).

If things go wrong

If there is a breach in security, such as an accidental unauthorised breach of data protection, contact the department's Information Security Representative who will assist with further procedures:

- ensure that the information is no longer available
- inform affected persons of the incident
- inform the UCPH Information Security Unit by filling in the form in the employee guide. The Information Security Unit will inform the Data Protection Agency about the incident within 72 hours of its being discovered if required.

OTHER USEFUL LINKS

- GDPR for Researchers
- GDPR and research projects
- Danish Data Protection Agency (in Danish)
- Guide in Data management of Personal data in Research/NEXS (English version in process)
- Employee guide: Handling of security incidents

ABBREVIATIONS AND GLOSSARY	
DDPA	Danish Data Protection Agency
DMA	Danish Medicines Agency
DPO	Data Protection Officer
EC	Committee on Health Research Ethics
EU	European Union
EØS (EEA)	The 28 EU countries plus Iceland, Liechtenstein and Norway
GDPR	EU General Data Protection Regulation
GCP	Good Clinical Practice
KU/UCPH	Københavns Universitet/University of Copenhagen
Pseudonymisation	"Pseudonymisation" means replacing any identifying characteristics of data with a pseudonym, or value, which does not allow the data subject to be directly identified. Pseudonymisation should be distinguished from anonymisation. It provides only limited protection of the identity of data subjects, as in many cases it still allows identification via indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing underlying or related data.
Pseudonymised data	Pseudonymised data remains personal data.
Anonymisation	"Anonymisation" of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. More specifically, data are anonymised when they do not allow individuals to whom they relate to be identified, nor is it possible for individuals to be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.
Anonymised data	Irreversibly and effectively anonymised data are not "personal data", so the data protection principles do not have to be complied with in respect of such data.
Data controllers	Data controllers can be either human persons or "legal persons" such as companies, governmental departments and voluntary organisations. All data controllers must comply with important rules governing their collection and use of personal information. They must also re-register annually in order to make their data handling practices transparent.
Data processor	The data processor is someone distinct from (working at a different university) the data controller for whom she/he is processing the personal data.

GDPR for Researchers

Authors: Data Quality Coordinator Lene Stevner, NEXS, SCIENCE, and Professor Peter Sandøe, IFRO, SCIENCE, and IVH, SUND/Sept. 2018, version 1.10

UNIVERSITY OF COPENHAGEN
DEPARTMENT OF FOOD AND RESOURCE ECONOMICS

ROLIGHEDSVEJ 25
DK-1958 FREDERIKSBERG C
DENMARK

TEL: +45 3533 6800
E-MAIL: IFRO@IFRO.KU.DK
WEB: WWW.IFRO.KU.DK

ISBN: 978-87-92591-98-2