



# Recommendations under data protection law for the preparation of a declaration of consent within the framework of research projects<sup>1</sup>

Participants in research projects have a right for the protection of their personal data. Participants must consent with the usage of their personal data. As a rule, this consent is given by means of a declaration of consent on the part of the research participants.

In the following, you will find information on how to prepare a declaration of consent, which results from the General Data Protection Regulation (GDPR). Details on your duty to inform study participants can be found in Art. 13 et seq. of the GDPR.

In addition, the declaration of consent must be in accordance with the research ethical guidelines of the German Psychological Society (DGPs), which are formulated in the professional ethical guidelines. The ethics committees do not check the correctness of your information on the responsible data protection officers and supervisory authorities. As a matter of principle, the ethics committee only examines data protection aspects of research projects on a cursory basis. The vote of the ethics committee does not replace the consultation of the responsible data protection officer. In particular, consult the data protection officer if you plan to process sensitive personal data.

In the following you will find general information on data protection consents and their legal basis. In the second part of the text you will find a sample with filling aids. At the end of the document you will find a list of the state data protection authorities.

## Part I: Principles of consent and information requirements

In the case of research projects, it can in most cases be assumed that there is no legal basis for collecting the data. It is therefore necessary for participants to give their consent to the collection of personal data.

---

<sup>1</sup> Based on the recommendations of the German Psychological Society (DGPs) (Version:09/2018)



According to Art. 4 No. 11 GDPR, "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;". Personal data (Art. 4, Para. 1 GDPR) means "[...] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

When researchers obtain data protection consent to collect personal data, they must also comply with the legal obligation to provide information. Examples can be found in the second part.

The following consent requirements must be fulfilled in principle:

1. Proof that a consent was given. The person responsible must be able to provide consent for the collection of personal data. A written form is not absolutely necessary, but it does make it easier to provide proof later. Consent can be obtained by signature in paper form or electronically. For the latter, § 126a BGB must be observed (name, qualified electronic signature<sup>2</sup>).

2. Naming of the person responsible

Best with letterhead, name of responsible person incl. complete address.

3. Informedness

The study participant shall be informed in detail in writing and in a manner understandable to him about the nature, extent and purpose of the collection and storage of personal data. If the processing serves several purposes, consent should be given for all processing purposes. Participants must be given the opportunity to ask questions. Consent must be given in clear and simple language. The consent must be clearly distinguishable from other facts. Consent must be given actively, e.g. by ticking options (opt-in procedure).

4. The consenting person must be at least 16 years old.

Parents/custodians must consent to the processing of personal data of children/young people up to the age of 16 (Art. 8 GDPR 2018).

5. Rights of the consenting party

The participants of a study have the right of objection, access, transferability, deletion, limitation of processing and rectification. These rights and the possibility of exercising

---

<sup>2</sup> A qualified electronic signature is a signature that is based on a qualified certificate at the time of signature and was created by a secure signature creation device.



them must be pointed out (name contact person with contact details).

## 6. Voluntariness

Participation in the investigation must be voluntary. Tying to other services or a contract is not permitted. A universal, unrestricted consent is also not possible. There must be a specific purpose for the data processing. The consenting party must have a "real" choice to refuse or withdraw consent without facing any disadvantages.

## What is to be considered when planning a study?

For example, the Bavarian State Commissioner for Data Protection has published an [information sheet on data protection in patient studies](#).

## Description of the workflow

A description of the collection and processing of personal data is essential for assessing data protection compliance. Typical aspects to be addressed (not an exhaustive list) include

- ✓ Inclusion of the study participants in a study
- ✓ Collection of data
- ✓ Possible collection of samples/creation of recordings
- ✓ Labelling of the samples/photographs
- ✓ Transmission of data and/or samples/photographs
- ✓ Scientific evaluation, publication of results
- ✓ Withdrawal of participation by the study participants, including data deletion, destruction of samples, information on stored personal data to participants
- ✓ Type and duration of data storage

## Quality assurance, monitoring

It must be specified who is authorized to access the data, how this access is carried out and which data may be accessed. If possible, only pseudonymised data should be accessed. Pseudonymisation means the processing of personal data in such a way that the personal data can no longer be attributed to a specific individual without additional information. The additional information must be kept separate from the pseudonymised data. Technical and



organisational measures must be taken to ensure that the personal data cannot be attributed to any individual.

If the data are anonymized (recital 26, sentences 6 and 6 GDPR), the GDPR is not applied. Anonymization requires that a test subject cannot be identified. Anonymous information is information that does not relate to an identified or identifiable natural person, or personal data that has been rendered anonymous in such a way that the data subject cannot be identified or can no longer be identified. The distinction between factual and absolute anonymization was abandoned in the GDPR.

If you plan to store the data on open-data servers, only use open-data servers (research data centers) for pseudonymised data, which limit the use to scientific purposes (scientific use). As an alternative to storage on an open-data server, you can also offer controlled remote data processing. A syntax created by researchers on the basis of test data sets is transmitted to the research data center and processed exclusively by local staff on the basis of the original data.

Pseudonymisation is considered insufficient if a combination of data (e.g. date of birth, gender, mother's name, subject of study, particularly outstanding features such as rare professions in combination with place of residence, etc.) makes it possible to identify the test subject.

## Technical design

- ✓ What technical means are used to collect and process data? How does electronic data collection work? (see also workflow)
- ✓ Description of the used databases and corresponding servers (where are the servers?) Who operates the software and has access to personal data?
- ✓ Description of the components for data suppliers and data retrieval (clients)
- ✓ Networking structure between the participating components
- ✓ Responsibilities for the components
- ✓ Applications, software used

## Technical and organisational security measures (TOMS)

The security of the data processing must be guaranteed and the measures taken must be described (§ 32 GDPR 2018). Among other things, this applies:

- ✓ Pseudonymisation and encryption of personal data.



- ✓ The ability to ensure the confidentiality, integrity, availability and resilience of the systems and services associated with the processing on a permanent basis.
- ✓ Rapidly restore availability and access to personal data in the event of a physical/technical incident.
- ✓ Regular review of TOMS for effectiveness procedure log.

You may need to create a procedure directory if your organization has not yet done so. A procedure directory is a list of all processing activities for personal data (see the work aid Procedure Directory).



## Part II: Samples with filling aids

### Important!

The text in italics is for information only and should be deleted. Sample formulations are formatted in black. Use the sample to create your own document for your consent, e.g. on your letterhead.

Please insert your own headers and footers and use your letterhead. Leave the page numbers.

### Data protection clarification and consent incl. information according to Art. 13 EU-GDPR

.....

Name of consenting party in block capitals

Date of birth .....

### 1. Detailed description of the research project

*Please describe your research project in detail in an easily understandable form. The participating person should get an idea of what is being investigated in the project. Ethically problematic behaviour (deception, etc.) does not play a role in data protection considerations, but it does play a role in the ethical evaluation of research. The study participants must be put in a position to weigh up the severity of the invasion of privacy.*

### 2. Content and purpose of the study

*The purpose shall be indicated in such a way as to provide an overview of the extent of the data collected. The data can only be used for the purpose of the research project. A later*

*"Re-dedication" is not possible.*

*Note: If the exact use of data is not yet known, research areas or projects should be identified. In principle, the purpose should be as broad as possible in order to avoid subsequent renewed consent to the collection of data. However, a blanket consent is not possible.*



*If several research areas exist, all must be listed and there must be an active possibility for selection (consent, rejection, opt-in, Art. 4 No. 11 GDPR).*

1. *Consent with Question 1*
2. *Consent with Question 2 etc.*

*If the responsible person for the data wishes to process the data for a purpose other than that for which they were originally collected and for which the consent was given, he/she must inform the data subjects of this further purpose before processing and obtain their consent for processing.*

### 3. Group of data subjects

*Group of targeted participants - Are there people who are not able to consent? Is information on other groups of people (e.g. partners, relatives, friends) also collected?*

### 4. Data to be collected

*What personal data is collected?*

### 5. Analysis results of the data

*Which analyses are obtained from the data or can potentially be obtained? Do the analyses yield any data worth protecting?*

### 6. Storage and transfer of data

*How is the data stored or passed on?<sup>3</sup>*

### 7. Participants, data flows and storage locations

*Who is involved in the study and how are the tasks distributed? Which bodies collect data and which bodies store it? What is passed on to whom and who has access to the data within the*

---

<sup>3</sup> If you plan to store the data on open-data servers, only use open-data servers (research data centres) for pseudonymised data, which limit the use to scientific purposes (scientific use). As an alternative to storage on an open-data server, you can also offer controlled remote data processing. A syntax created by researchers on the basis of test data sets is transmitted to the research data center and processed exclusively by local staff on the basis of the original data.



*scope of the research tasks (possibly with reference to patients or to the usually pseudonymised/anonymised research data)? Who assumes responsibility for compliance with data protection?*

*Attention: in the case of international studies, it must be checked whether data is stored by subcontractors/cooperation partners, how they store the data or whether only central access to data- protection-secure servers is possible. Is data stored in third countries? Please note that data flows at institutions of your university can also be external bodies in terms of data protection (e.g.: affiliated institutes, outpatient departments, clinics, computer centres, etc.).*

Recipient 1 (name, address): .....

Data: .....

Recipient 2 (name, address): .....

Data: .....

## **8. Concrete duration of storage**

*Specify the duration of the data storage. Will they then be deleted/blocked/anonymised (deletion of assignment key)? What happens to data stored by third parties? Is there a legal basis for the duration of storage?*

## **9. Pseudonymisation procedure**

*Place of pseudonymisation; description of the overall process; administration of the assignment of pseudonym - test person data*

## **10. Legal basis**

*What is the legal basis for data collection? In most cases, this is the consent of the participants (participant information and declaration of consent). Consent to the processing of personal data should be given in writing for reasons of verifiability.*





*Sample text:*

*The legal basis for the processing of the personal data mentioned is the consent according to Art. 6 (1) letter a EU- GDPR in the second part of this document.*

## **11. Revocation by the party concerned**

*Point out the right of withdrawal at any time (Art. 21 GDPR). Please state that the revocation does not affect the lawfulness of the processing carried out until the revocation (revocation with effect for the future, Art. 7, Para. 3 DSGVO). What happens to data transferred to third parties in the event of revocation? (Note: Data which have already been included in statistics etc. within the scope of research can generally not be removed retroactively). The revocation must be as simple as the consent.*

*What else happens in case of revocation? E.g. in the case of research: is participation in the study thus terminated?*

*Sample text:*

*You have the right to revoke your data protection consent at any time. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of consent until revocation. (Revocation with effect for the future).*

*Please address the revocation to the responsible person.*

*If applicable: You will not suffer any disadvantages as a result of the revocation (if necessary, mention the consequences of the revocation).*

*If possible: After receipt of the revocation, the personal data will be deleted / blocked / anonymised. (Please delete as applicable)*

## **12. Name, contact details of the responsible person**

*In the sense of the GDPR, this is usually the president, rector of the university or head of the research institution. Please contact your data protection officer to find out who assumes responsibility at your institution. The person responsible within the meaning of the GDPR is a natural or legal person, authority or institution or other body which alone or jointly with others decides on the purposes and means of the processing of personal data (Art. 4, para. 8, GDPR, definitions). A distinction must be made between the data controller and the data subject. This is a person who has initiated or manages the data processing.*

*Responsibility for the processing of personal data lies with the data controller: Please enter your contact details here.*



### 13. Contact details of the data protection officer

Herr Jörg Flierenbaum

Würzburger Straße 23

97230 Estenfeld

E-Mail: [datenschutzbeauftragter-srh@symbion-ag.de](mailto:datenschutzbeauftragter-srh@symbion-ag.de)

### 14. Reference to the rights of data subjects

Pursuant to Art. 13 Para. 2 lit. b of the Basic Data Protection Regulation, you have the right for

- / Information (Art. 15 GDPR and §34 BDSG)
- / Opposition (Art. 21 GDPR O 2018 and §36 BDSG)
- / Data transferability (Art. 20 GDPR)
- / Deletion (Art 17 GDPR and §35 BDSG)
- / Limitation of processing (Art 18 GDPR) Correction (Art 16 GDPR)

If you wish to exercise any of these rights, please contact the person responsible.

*Enter research institution incl. address, phone, e-mail.*

You also have the right to lodge a complaint with the supervisory authority:

*Enter the relevant state authority for data protection with contact details*



## 15. Consent to the collection and processing of personal data

I hereby voluntarily consent to the collection and processing of my personal data. I have been sufficiently informed and had the opportunity to ask questions. I have been informed about the consequences of a possible revocation of my data protection consent at any time. I have been informed that by withdrawing my consent, the lawfulness of the processing carried out on the basis of the consent until revocation is not affected.

I have received the written clarification and consent.

.....  
Place | Date

.....  
Signature of person affected

.....  
Signature of person having custody



## Address list of the Data Protection Officers of the states and the federal government

The following addresses are taken from the [websites of the Federal Commissioner for Data Protection and Freedom of Information](#) (accessed on 12.06.2019). Addresses of the international data protection commissioners can also be found there.

### Federal government

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit  
Husarenstr. 30  
53117 Bonn  
Phone: +49 228 997799 0  
E-Mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)  
Website

### *Baden-Württemberg*

Dr. Stefan Brink  
Postfach 10 92 32  
70025 Stuttgart  
Phone: +49 711 615541 0  
E-Mail: [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de)  
[Website](#)

### *Bavaria*

Dr. Thomas Petri  
Postfach 22 12 19  
80502 München  
Phone: +49 89 21 26 72 0  
E-Mail: [poststelle@datenschutz-bayern.de](mailto:poststelle@datenschutz-bayern.de)  
[Website](#)

### *Berlin*

Maja Smoltczyk  
Friedrichstraße 219  
10969 Berlin  
Phone: +49 30 138 89 0  
E-Mail: [mailbox@datenschutz-berlin.de](mailto:mailbox@datenschutz-berlin.de)  
[Website](#)



### *Brandenburg*

Dagmar Hartge  
Stahnsdorfer Damm 77  
14532 Kleinmachnow  
Phone: +49 332 03 356 0  
E-Mail: [poststelle@lda.brandenburg.de](mailto:poststelle@lda.brandenburg.de)  
[Website](#)

### *Bremen*

Dr. Imke Sommer  
Arndtstraße 1  
27570 Bremerhaven  
Phone: +49 421 361 2010  
E-Mail: [office@datenschutz.bremen.de](mailto:office@datenschutz.bremen.de)  
[Website](#)

### *Hamburg*

Prof. Dr. Johannes Caspar  
Klosterwall 6 (Block C)  
20095 Hamburg  
Phone: +49 40 428 54 40 40  
E-Mail: [mailbox@datenschutz.hamburg.de](mailto:mailbox@datenschutz.hamburg.de)  
[Website](#)

### *Hesse*

Prof. Dr. Michael Ronellenfitch Gustav-Stresemann-Ring 1  
65189 Wiesbaden  
Phone: +49 611 140 80  
E-Mail: [poststelle@datenschutz.hessen.de](mailto:poststelle@datenschutz.hessen.de)  
[Website](#)



*Mecklenburg-Western Pomerania*

Heinz Müller  
Lennéstraße 1  
Schloss Schwerin  
19053 Schwerin  
Phone: +49 385 59494 0  
E-Mail: [info@datenschutz-mv.de](mailto:info@datenschutz-mv.de)  
[Website](#)

*Lower Saxony*

Barbara Thiel  
Prinzenstraße 5  
30159 Hannover  
Phone: +49 511 120 45 00  
E-Mail: [poststelle@lfd.niedersachsen.de](mailto:poststelle@lfd.niedersachsen.de)  
[Website](#)

*North Rhine-Westphalia*

Helga Block  
Kavalleriestraße 2-4  
40213 Düsseldorf  
Phone: +49 211 384 24 0  
E-Mail: [poststelle@ldi.nrw.de](mailto:poststelle@ldi.nrw.de)  
[Website](#)

*Rhineland-Palatinate*

Prof. Dr. Dieter Kugelmann  
Postfach 30 40  
55020 Mainz  
Phone: +49 6131 208 24 49  
E-Mail: [poststelle@datenschutz.rlp.de](mailto:poststelle@datenschutz.rlp.de)  
[Website](#)



### *Saarland*

Monika Grethel  
Fritz-Dobisch-Straße 12  
66111 Saarbrücken  
Phone: +49 681 947 81 0  
E-Mail: [poststelle@datenschutz.saarland.de](mailto:poststelle@datenschutz.saarland.de)  
[Website](#)

### *Saxony*

Andreas Schurig Bernhard-von-Lindenau-Platz 1  
01067 Dresden  
Phone: +49 351 49 3 5401  
E-Mail: [saechsdsb@slt.sachsen.de](mailto:saechsdsb@slt.sachsen.de)  
[Website](#)

### *Saxony-Anhalt*

Dr. Harald von Bose  
Postfach 19 47  
39009 Magdeburg  
Phone: +49 391 818 03 0  
E-Mail: [poststelle@lfd.sachsen-anhalt.de](mailto:poststelle@lfd.sachsen-anhalt.de)  
[Website](#)

### *Schleswig-Holstein*

Marit Hansen  
Postfach 71 16  
24171 Kiel  
Phone: +49 431 988 12 00  
E-Mail: [mail@datenschutzzentrum.de](mailto:mail@datenschutzzentrum.de)  
[Website](#)




*Thuringia*

Dr. Lutz Hasse  
Postfach 90 04 55  
99107 Erfurt  
Phone: +49 361 57 311 29 00  
E-Mail: [poststelle@datenschutz.thueringen.de](mailto:poststelle@datenschutz.thueringen.de)  
[Website](#)

*ULR directory*

[DSGVO 2018](#)

 Professional ethics guidelines

Electronic Signature