TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.

Manual for writing a data protection concept

Translated from the german version 1.0 of December the 12th, 2017
„*Checkliste zur Erstellung eines Datenschutzkonzeptes*“
Written by Antony G, Bialke M, Pommerening K and Repp R

The present manual is based on the TMF Working group's many years of experience in data protection. The checklist was compiled using selected contents from:

1. data protection concepts of the *MOSAIC project* from the *Institute for Community Medicine* of *University Medicine Greifswald* (*ICM*) [(I)],
2. guidelines for the creation of data protection concepts in health care of the working group on data protection of the German Association *for Medical Informatics, Biostatistics and Epidemiology* (*GMDS*)[(II)],
3. the Standard Data Protection Model (SDM) of the 92nd *Conference of the Independent Data Protection Authorities of the Federal Government and the federal states*[(III)],
4. the current Recommendations 2017 on Data Protection and Research Data of the *Council for Information Infrastructures* (*RFII*)[(IV)],
5. requirements resulting from recent amendments to the Federal Data Protection Act (BDSG)[(V)] due to the new EU Data Protection Regulation (EU-GDPR)[)(VI)]. Please note, that not all relevant provisions by the GDPR are fully integrated in this manual, since the update of the TMF Data Protection Guideline with respect to the GDPR is not yet completed.In particular the role and necessity of conducting a DPIA is not explicitly covered.

This manual will provide short and clear information on questions concerning data protection concepts and necessary accompagnying documents.Moreover it will serve as a guide to the relevant parts of the TMF's Data Protection Guideline that has been published in the TMF publication series (in german – a translation to English is in progress):

> K. Pommerening | J. Drepper | K. Helbing | T. Ganslandt. **Leitfaden zum Datenschutz in medizinischen Forschungsprojekten.** Generische Lösungen der TMF 2.0. 2014. [ISBN 978-3-95466-123-7]

This guideline is supplemented by the generic data protection concept for biobanks, which is published as volume 6 of the TMF publication series:

> Becker, R., Ihle, P., Pommerening, K., Harnischmacher, U. **Ein generisches Datenschutzkonzept für Biomaterialbanken** (Version 1.0). 2006. TMF. http://www.tmf-ev.de/produkte/P010021 (Abruf: 2017-11-01)

This manual is not necessarily intended as a template for a data protection concept, but serves primarily to provide guidance, how such a concept could look like and to check whether relevant aspects have been considered.

references [I] to [VI] at the end of this document

Content

What is a data protection concept?

Medical research almost inevitably interferes with the constitutionally guaranteed personal rights of the affected people - patients or test persons. This intervention is justified and accepted *within certain limits* by the society's benefits of medical progress and by the freedom of science also assured by the constitution of the federal republic of Germany. However any restrictions must be compensated by particularly careful protective measures.

The data protection concept of a medical research project specifies the *necessity* and *appropriateness* of the data processing and describes all measures that contribute to the effective protection of personal rights.

In order to **justify the necessity** of law interferences, the research objective, the data sampling, and bio sample collection must be described as explicitly as possible.

The **description of measures** addresses the effectiveness of the protection of personal rights, and in particular of personal data, as well as the minimisation and control of the re-identification risks. It specifies organisational regulations and technical measures for IT security.

The **description of appropriateness** comprises the reason why the research objective can be achieved in this way but not with less personal right interferences, as well as a consideration of the appropriateness of the protective measures. In addition it also includes the reason as to where personal data must be available, where pseudonymisation is appropriate, and where anonymised data are sufficient.

In order to be able to formulate a data protection concept, the author has to be clear on:

- the project objectives and the approach to achieve them, including the appropriate scientific methodology,
- the organisational structures, processes, and communication channels of the research project or network (including planned biobanks or sample storage),
- the IT concept: use cases to be covered by IT as well as data, data flows, and intended data usage,
- the intended implementation of the IT architecture and data storage

Some general, fundamental, and specific questions about a data protection concept are answered in the FAQ on data protection (in german):

http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS/FAQsDatenschutz.aspx

Preparation of a data protection concept and evaluation

The basis for the creation of a data protection concept for a medical research project is the comprehensive TMF guideline, which describes generic data protection concepts for various scenarios.

If a data protection concept has been prepared in accordance with the TMF guideline and deals with the individual points of this checklist, the TMF Data Protection working group can provide a written vote confirming accordance with the guideline. This vote can be submitted:

- to the statutory consultation and examination by the responsible official or company data protection officer,
- as certificate for the data protection impact assessment in the sense of the GDPR[1],
- during an examination by the data protection supervisory authority (e.g. when examining the description of the procedure in the processing overview)[2],
- during the examination of the ethics proposal

The main steps for obtaining such a vote are described (in german) in the document "Information on the Advisory Service"; http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS/Beratung.aspx

A data protection concept comprises a number of additional documents which should be submitted to TMF-Data Protection working group or explained in more detail in the data protection concept with regard to their regulatory content:

- Information for patients / test persons and the form for the informed consent
- Cooperation agreements and contracts between project partners
- Contracts with consultants
- Conditions and requirements for the receipt of grants
- Internal guidelines, policies and SOPs
- IT security concept (with a more detailed description of the measures which are only briefly listed in the actual data protection concept)

These may be separate documents or attachments. The legal correctness of these documents is not evaluated by TMF -Data Protection working group.

[1] Art. 35, 36 GDPR in conjunction with § 67 BDSG

[2] Art. 30 GDPR

I. Presentation of the research project

The research project should be described and its necessity justified. The benefits of the project, also for the persons concerned, should be described.

- What is the aim of the research project and how should it be achieved?
- What progress in science is being achieved, or what is the expected benefit?
- How does this research project distinguish itself from similar projects?
- How are treatment and research contexts delimited within the framework of the research project?
- Which research questions have already been formulated or will be pursued in the future?
- What positive effects can be achieved for the quality of treatment?
- What justifies the interference with the fundamental right of natural persons to the protection of their personal data?
- Are there definable phases of the research project, e.g. a pilot phase with simplified measures for a limited period of time?
- Doe plans for a gradual expansion of the research project exist, for whose subsequent stages the concept can or should be specified later?
- What is the design of the research project (e.g. study design)?
- Is the goal of the research project achievable?
- Which scientific, especially biostatistical methods should be applied?
- How are methodicians/biostatisticians/computer scientists involved?
- To what extent can anonymised or pseudonymised data be used, or in which processes is an explicit personal reference unavoidable?
- How long is the planned duration of the research project?
- Is the continuation of the research project regulated even after the current project funding has expired?

I. Organisational structure

The persons and organisations involved or to be involved in the project, their relationships with each other and their areas of responsibility should be described.

A. Responsible data processor

- Regarding the GDPR, who is responsible for the personal data or bio samples[3] (e.g. university/institute/clinic or other organisation)?
- What is their legal status (e.g. institution or corporation under public law, public foundation, company under private law)?
- What is the research focus of the responsible processor?

B. Participants, cooperation partners, joint data controllers?

- Which other organisations, partners and institutions are involved?
- Are there several responsible persons[4]? If so, who fulfils which obligation in respect to the EU- GDPR? What is their legal status?
- What are the reasons for the participation of cooperation partners or service providers and which functions or tasks do they have within the research project?
- How are the areas of responsibility defined? (Who is involved in which way and who is responsible?)
- How is the cooperation within the research project regulated (e.g. rules of procedure, statutes, cooperation agreements, shareholders' agreement, on a legal form)?
- Which governing body and other decision-makers are planned (e.g. executive board, general meeting, shareholders' meeting or management)?
- In which role and function are special societies and patient organisations involved?

C. Organisational dependencies

- Which entities of the research project act as independent partners?
- Who is the consultant or service provider (e.g. for hosting)?
- What are the possible conflicts of interest?
- Which trustee services (data trustee, trust office) should be integrated (e.g. medical informatics institute, internal data protection officer, external company, or notary)? Reason for suitability?

[3] cf. Art. 4 para. 7 GDPR 2016/679
[4] cf. Art. 26 GDPR 2016/679

- How is the separation of informational powers specifically regulated? (e.g. data distribution matrix showing which partner has access/knowledge to what kind of information.)

Place holder

Insert

Organisation Chart

D. International aspects

- Which foreign project partners are involved?
- Are contracts awarded abroad (e.g. for laboratory tests)? If so, what is the legal basis?
- Is the use of personal data and/or bio samples by foreign parties intended? If so, on what legal basis should personal data and/or biomaterial samples be transferred abroad (e.g. EU area, European commission adequacy decision[5], appropriate guaranties[6] if necessary[7] with the approval of the data protection supervisory authority)?

E. Finances of the research project

- Who funds the research project and for how long (e.g. basic funding, temporary project funding, contract research)?
- What type of continuation is planned after the current funding has expired?
- To which sponsorship should personal data and bio samples be transferred in the long term, or how will personal data and/or bio samples be handled after the end of the funding period?

[5] cf. Art. 45 GDPR 2016/679
[6] Art. 46 GDPR
[7] cf. Art. 46 GDPR 2016/679

II. General conditions relevant to data protection

The planned project processes with their organisational and legal conditions should be presented.

A. Application/use cases

Operation	Explanation
Obtaining Informed consent	…
Collect data and/or bio samples	…
Recruiting participants	…
Transfer of data and/or bio samples	…
Storage of data and/or bio samples	…
Providing data and/or bio samples	…
Conducting follow-ups	…
Withdrawal of informed consent	…

Exemplary overview of workflows

B. Basic framework conditions

- Which general data protection law applies to the responsible processor in addition to the GDPR (*Federal Data Protection Act, State Data Protection* Act)?
- Is the research project subject to relevant special laws (e.g. cancer register laws, pharmaceutical law, Code of Social Law, social security codes (SGB), federal registration law)?
- Should personal data from other sources with special legal conditions be used (e.g. secondary use of routine data, reporting data)?
- Are there any state-specific regulations for the secondary use of treatment data (e.g. State Hospital Laws)?
- Should personal data and/or bio samples from the treatment documentation be used for the research project or transferred from the research project to treatment documentation (release from confidentiality, data transfer permit)?
- Is a direct retroactivity on the treatment of individual patients or test persons to be expected or conceivable?

C. Scope of data processing and bio sampling for the planned research project

- Which persons/groups of persons are affected by the planned data processing (patients and test persons, relatives, employees of participating institutions, employees of non-participating institutions such as treating physicians etc...)?
- Does the research project concern children[8] in respect of the GDPR?

[8] cf. Art. 8 GDPR 2016/679

- Does the research project concern vulnerable persons or groups of persons (e.g. persons unable to give consent)?
- How are inclusion and exclusion criteria for test persons defined?
- What personal identifying data should be processed?
- What personal medical data should be processed?
- Should biomaterials be collected and, if necessary, stored?
- What kinds of biomaterial samples are required?
- What special categories of personal data[9] within the GDPR should be processed?
- Should identifying personal or medical data and/or bio samples from other own research projects be used or made available by other institutions (e.g. biobank)? If so, by which institution and on what legal basis will this be done (e.g. declaration of informed consent, change of purpose, data usage agreement or material transfer agreement)? How are the information[10] responsibilities[11] according to the GDPR fulfilled?
- Should or must suppliers of personal data and/or bio samples retain or have to retain access to the data or must personal data be disclosed to these suppliers (e.g. random findings or other analysis results within the research project)? If so, on what legal basis will this be done?
- Which collection area and which case numbers are planned for the research project?

D. Collection of personal data and/or bio samples

The desired collection of personal data and/or bio samples shall be described.

- How will personal data and/or bio samples be collected in detail?
- Who is responsible for informing test persons and obtaining an informed consent?
- Who collects personal data and/or bio samples? Are any partners involved in the collection of personal data and/or bio samples?
- How is the quality standard of the personal data assured during the collection (e.g. plausibility and completeness checks)?
- How large is the estimated data volume?
- How often is personal data of an individual collected (follow-ups)?

[9] cf. Art. 9 in conjunction with Art. 3 para. 13 ff GDPR 2016/679
[10] cf. Art. 14 GDPR 2016/679
[11] Art. 14 GDPR

E. Data integration and storage of personal data

The storage of personal data is to be described.

- How is personal data stored in detail?
- Where is what personal data stored?
- How is personal data stored (e.g. centralized, decentralized, paper-based, file-based, database, data warehouse)?
- Is the personal data anonymised or pseudonymised before or during storage? (for technical procedures see VII H)
- How is the multi-centrally collected personal data merged?
- How is heterogeneous personal data merged?
- Is the personal data versioned or documented with an audit trail procedure?

F. Storage of bio samples

- At which location(s) are the bio samples stored and for how long?
- How are the bio samples stored (central or distributed biobank)?
- Should a project specific biobank be established or used?

G. Use of personal data and/or bio samples

- What is the primary and/or secondary purpose for personal data and/or bio samples (e.g. for observational studies, hypothesis generation/data mining, recruitment for future clinical or epidemiological studies, translational research, medical quality control)?
- To what extent can future secondary use already be limited, and to what extent should it remain open?
- Who should be allowed to use personal data and/or bio samples?
- Will personal data and/or bio samples be transferred to other internal and/or external research projects?
- In what form will personal data and/or bio samples be made available to third parties?
- Is there a standardized application procedure for using personal data and/or bio samples internally or externally? Who decides on these applications?
- Which steps (e.g. re-identification/anonymisation) are necessary for the transfer of personal data and/or bio samples to third parties?
- Is a feedback of analytical results to the bio sample distributor or a return of the bio sample necessary?

H. Anonymisation and deletion of personal data and/or destruction of bio samples

- Are personal data deleted or made anonymous after the death of test persons?
- Are there any standard time periods for the deletion of personal data?
- Are comparative samples of the bio sample, that has been used for scientific publications, archived? If so, where and how have they been stored?
- How are personal data for scientific publications stored?

III. Basic principles for the protection of the rights and freedoms of the persons concerned

The basic considerations on data protection in the terminology of data protection legislation shall be presented.

A. Lawfulness, fairness, transparency[12]

- Is a written informed consent required from test persons or is the processing of personal data and/or bio samples carried out on the basis of a legal regulation? If so, on what legal basis?
- What is the procedure for natural persons with limited or no consent (e.g. children)?
- Are there any requirements from patient organisations or ethic committees regarding the education of volunteers and on the informed consent?
- To what extent is a separate release from legal confidentiality required?
- Is the pseudonymous processing of personal data and/or bio samples covered by the informed consent?
- Is anonymisation of personal data covered by the informed consent?
- What additional transparency measures will be put in place for the research project (e.g. public relations, website or publication rules)?

B. Appropriation[13]

- How broad is the informed consent formulated? Is it a broader, a detailed, or appropriated informed consent?
- Are there any gradations or clear options for the informed consent?
- Is re-contacting of test persons covered by the informed consent (e.g. in the case of random findings or follow-ups)?

[12] cf. Art. 5 para. 1 lit. a GDPR 2016/679

[13] cf. Art. 5 para. 1 lit. b GDPR 2016/679

C. Accuracy[14]

- Is the informed consent checked for completeness and, if necessary, partial deletions? When is a valid informed consent available?
- How is it ensured that personal data is correctly collected and can be corrected or deleted at a later stage?

D. Restriction to the possessing of data[15]

- How is it ensured that only personal data and/or bio samples relevant and necessary for the research purpose are processed?
- Are personal identifying data that are no longer required deleted?

E. Integrity and confidentiality[16]

- How is it ensured that personal data and/or bio samples are protected from unauthorized or unlawful processing?
- How are personal data and/or bio samples protected against loss, destruction or damage?

F. Risk assessment of the rights and freedoms of natural persons

- Should processes [17] be established or used to conduct a data protection impact assessment and who is involved?
- Has the operational or regulatory data protection officer been involved in assessing the risks to the rights and freedoms of the data subject? Has he/she also assessed the appropriateness of the proposed technical and organisational measures?
- Has processing of personal data and/or bio samples been systematically described? Is the proposed processing well justified by the purposes and the interest pursued by the controller?
- Is there a detailed assessment of the necessity and proportionality of the proposed processing for the research project?
- Have any risks to the rights and freedoms of data subjects resulting from the proposed processing of personal data and/or bio samples for the research project been identified? Has the likelihood of the risks identified been assessed?
- Have appropriate and demonstrably effective organisational and/or technical measures been identified that adequately mitigate the identified risks to the rights and freedoms of the data subjects?
- Where appropriate, have the views of the data subject or their representatives (e.g. patient organisations) been obtained?

[14] cf. Art. 5 para. 1 lit. d GDPR 2016/679

[15] cf. Art. 5 para. 1 lit. e GDPR 2016/679

[16] cf. Art. 5 para. 1 lit. f GDPR 2016/679

[17] cf. Art. 35 GDPR 2016/679

- Have appropriate processes been put in place to monitor or verify the effectiveness of changes in the risks associated with the processing of personal data and/or bio samples?

IV. Rights of the data subject

- Who is the contact person to exercise the rights of the data subject?
- How and where are the contact details of the contact person for data subject rights published and communicated?

A. Transparency

- How is it ensured that personal data and/or bio samples are processed lawfully, fairly and in a manner understandable to the data subject?

B. Duty to provide information when personal data and/or samples of biomaterial are collected from the test persons

- Is information provided in a timely and complete manner (pursuant to Art. 13 GDPR in conjunction with § 32 Federal Data Protection Law (BDSG))? Are there justified exceptions to the information requirements?
- How are the information obligations[18] fulfilled (according to the GDPR)?

C. Duty to provide information if personal data and/or biomaterial samples are not collected from the test person

- Is information provided timely and complete according to Art. 14 GDPR in concordance with § 33 Federal Data Protection Law (BDSG)? Are there justified exceptions to the information requirements?
- How can data subjects obtain information about their processed personal data and/or bio samples?
- How can data subjects obtain a copy of their processed personal data that concern them?
- Is information provided in accordance with Art. 15 GDPR in connection with § 34 Federal Data Protection Law (BDSG) complete? Are there justified exceptions to the information requirements?
- Which processes are effective for requests for information from affected data subjects? Who is involved?

D. Deletion and right to be forgotten

- How can data subjects exercise their right to deletion of personal data and/or destruction of bio samples?
- How does the deletion of personal data or the destruction of bio samples take place in detail? Are there justified exceptions to the obligation to delete?
- Are personal data deleted after the death of the data subject?
- Are there standard time periods for the deletion of personal data?

[18] cf. Art. 13 GDPR 2016/679

- How are personal data used for scientific publications stored?
- How is the right to deletion enforced if personal data have been made public? [19]

E. Limitation of processing[20]

- How can data subjects exercise their right to limit the processing of personal data and/or bio samples that concern them?
- How is the processing of personal data and/or bio samples restricted in detail? Are there justified exceptions to the obligation to limit processing?
- How will the data subject be informed of the removal of the processing restriction of their personal data and/or bio samples?

F. Data transferability[21]

- How can data subjects exercise their right to data portability of personal data and/or bio samples?

G. Objection to processing[22] and withdrawal of consent[23]

- How can data subjects exercise their right to object to the processing of personal data and/or bio samples?
- How can they object to the processing of personal data and/or bio samples in detail? Are there justified exceptions to the obligation to object?
- How can data subjects revoke their informed consent (e-mail, telephone, fax, in person, complete revocation or partial revocation)?
- Who processes informed consents to object to the processing of personal data and/or bio samples and to revoke the informed consent?
- Where are statements to object or withdraw to the processing of personal data and/or bio samples documented, recorded and stored?
- How are statements on objections or withdraw to the processing of personal data and/or bio samples enforced against third parties?
- What are the consequences of declarations to object or withdraw to the processing of personal data and/or bio samples (deletion, destruction, blocking, anonymisation, restriction of use)?
- Can objection and revocation be withdrawn? What happens in such a case?

[19] cf. Art. 17 para. 2 GDPR 2016/679

[20] cf. Art. 18 GDPR 2016/679

[21] Art. 20 GDPR

[22] cf. Art. 21 especially para. 6 GDPR 2016/679

[23] cf. Art. 7 para. 3 GDPR 2016/679

V. Organisational measures

The organisational measures (responsibilities, obligations and processes relevant to data protection) in the project are to be described.

A. Committees and functions

- Who constitutes the governing body (members as role or person)? What are its tasks?
- Who performs the functions of the Data Protection Committee (e.g. as use and access Committee) (members as role or person)? What are their tasks?
- Who belongs to which advisory board?
- Has an operational or official data protection officer been appointed and can their contact details be viewed by the data subjects?
- Has an IT security officer been appointed?

B. Internal regulations

- Is something relevant to the research project regulated in statutes or articles of association?
- Which guidelines (policies) and service instructions (SOPs) apply to employees of the research project?

C. Access rules

- What roles can employees have in the research project?
- Which rights belong to the respective roles? Who can see, enter, change or delete which personal data? Who has what kind of access to bio samples?
- What kinds of role conflicts can occur and how are they resolved?
- How are access rights monitored or enforced?

D. Data Trusteeship

- How is the independence of a data trustee service guaranteed?
- How is the transfer of functions of the data trusteeship regulated?
- To what regulations is the Data Trustee Service bound?

E. Use of Personal data and bio samples

- Is the informed consent obtained on paper or in electronic form?
- How long is an informed consent valid? Does it expire automatically?
- Is the informed consent obtained again? (e.g. follow-ups)
- How, where and for how long is an informed consent stored?
- Who is responsible for the administration of consent forms?

- Which processes apply in the event of an objection to the handling of personal data and/or bio samples of data subjects? Who is involved?
- Who is responsible for carrying out the individual processes of pseudonymisation, anonymisation, restriction and deletion of personal data and/or bio samples?
- Which processes apply in the event of a request to restrict the processing of data subjects? Who is involved?
- Which processes apply in the event of a request for deletion by the data subjects? Who is involved?
- Is it necessary to inform data subjects after these procedures have been carried out? Who is responsible for it?
- How is the use of personal data and/or bio samples basically regulated (e.g. only internal use, anonymous export, access with conditions, data evaluation only on site with publication of results)?
- Who decides on the use of personal data and/or bio samples in individual cases and on request?
- What requirements are associated with the use of personal data and/or bio samples? Where are those requirements regulated and agreed on (e.g. acceptance of usage regulations, data usage agreement, material transfer agreement)?
- Are there any contractual provisions (e.g. data usage agreement) with the data recipient which regulates the renewed transfer of personal data, the storage period and attempts to re-identify data subjects?
- Are there any contractual provisions (e.g. material transfer agreement) between the providing institution and the recipients of bio samples which regulate the renewed transfer of bio samples, the storage and prohibition of tests for the re-identification of the data subject?
- Who is responsible for or involved in the process of providing personal data and/or bio samples?
- What processes are involved in a request for data transfer of personal data and/or bio samples from affected persons? Who is involved?
- How is the data transfer of personal data and/or bio samples carried out in detail?

F. Monitoring procedure

- Is there a monitoring procedure and what does it look like (e.g. monitoring manual)?
- Who is intended as a monitor?
- How does monitoring work?
- What data does the monitor see and what processing rights does the monitor have (e.g. locking, deleting)?

G. Data quality assurance

- How are quality assurance measures integrated into the individual work and how are they effectively monitored?
- Which data quality assurance procedures are planned for the research project?
- Will a data quality manager be provided for the research project? If so, which personal data can he/she view?
- What special data protection requirements result from the data quality assurance procedure with regard to the re-identification of data subjects, feedback to data subjects and data collection?

H. Internal audit procedure

- Is there an internal audit procedure and what does it look like (description)?
- Who controls the technical and organisational security measures?
- Who is responsible for configuring the audit trail mechanisms?
- Where are procedures and processes documented?
- What is recorded in each case?
- Who has access to these audit logs?
- What powers/ rights does an auditor have?
- Are security audits carried out on a case-by-case basis or regularly (how often concretely)?
- Are audits carried out randomly or completely? How does the procedure work?
- To what extent are accesses both to the personal data and to the data storage systems logged?
- Is specific software used for this purpose? If so, what exactly and for what reason?
- How long are log files stored?[24]

I. Evaluation of personal data

- Who is responsible for evaluating the data?
- How is the data evaluated?
- Is the data pseudonymised or anonymised for evaluation?

J. Spatial measures

- What spatial measures are necessary from the point of view of data protection?
- How are the premises protected?
- Who has access to the premises?
- Who grants access rights?

[24] according to recommendations of the BSI IT Baseline Protection Catalogue[vii]

K. Personnel measures

- Are the employees involved in the research project bound to data secrecy and instructed?
- What personnel measures are necessary from the point of view of data protection?
- How do these measures fit into the hierarchy of the data controller?
- Have the employees involved in the research project completed a data protection training course? Are separate training courses necessary within the framework of the research project (e.g. on SOPs)?
- How are SOPs monitored? What happens if SOPs are violated?

L. Violations of the protection of personal data

- What measures should be put in place to detect breaches of personal data protection?
- How should it be ensured that this violation can be reported to the competent data protection supervisory authority within the statutory period of 72 hours?
- What processes have been put in place to notify data subjects of breaches of personal data protection and who is involved and how?
- Has an emergency plan been developed that covers all aspects of these notifications?

VI. Technical measures

From the point of view of IT implementation; describe the design of measures for the compliance with data protection requirements.

A. System components

- Which modules of the TMF concept are relevant?
- Which registers, biobanks including biomaterial management, study databases, image databases, research databases and analysis databases are planned?
- In the case of a registry, has it been decided whether it should be located in the clinical module or in the research module? (The following table lists the similarities and differences between the two modules as a decision-making aid.) Note: A large collaborative project may include several registries of different types.
- In the case of a biobank, has it been decided whether a clinical database or a research database is more suitable for the storage of annotation data (see glossary)? (The following table can also be used as a decision-making aid for this purpose.)
- In the case of an image database, has it been decided whether it should be part of the clinical module or the research module or whether a separate image data module should be set up? (The following table also serves as a decision-making aid for this.)

Clinical module	Research module
General data protection and medical confidentiality regulations	General data protection regulations, pertinent special laws if applicable (e.g. Cancer Registry Law)
Long-term data retention	Long-term data retention
Open research approach	Open research approach
Research and treatment interlinked	Research and treatment clearly separated
Data input/transfer from treatment context	No online access from treatment context, often additional data collection, e.g. “sociodemographic” data

B. System model

Data (-categories), processes, data flows and storage shall be described in such a way that the IT architecture becomes clear. This helps with identifying necessary data protection and IT security measures.

- Is there a description or categorisation of the data to be collected?
- Which data categories, formats and types should be used?
- Are there heterogeneous, homogeneous and/or unstructured data types?
- Are the processes described with the necessary details to justify the IT architecture and to identify necessary data protection and IT security measures?
- How should personal data be distributed under the aspect of separation of powers? How does the data flow between different modules and components work?
- What central/connecting components are required (e.g. rights management, data quality assurance, respondent management, contact management, identity management, pseudonym management, consent management)?
- Where should system components be located logically and physically? Under whose responsibility?
- What role do these components play in the processes of the research project? (A tabular representation of the components and processes would be helpful here, e.g. pseudonymisation, re-pseudonymisation, confidentiality, data quality assurance, revocation, deletion)
- What can a graphical representation of the entire data flow look like in detail?

C. Technical infrastructure

- Which Software should be used (e.g. database, EDC system, sample administration, pseudonym administration, consent administration, person administration)?
- Which servers should be operated? At which locations?
- Which external services should be used? (What about the multi-client capability of these services?)

D. Authentication and authorisations

The technical procedures used shall be described and their implementation described.

- Which authentication procedure is used?
- Has the authorization procedure been described (role and rights control)?
- For which areas is the rights /role concept valid?
- Which roles exist and which rights are associated to them (tabular overview, if applicable)?
- Who is responsible for assigning roles and rights?
- How is access controlled?
- What measures are planned to be able to subsequently check and determine whether and by whom personal data have been viewed, entered, changed or deleted (e.g. by logs)?
- How are the logs handled?

E. Securing the network (IT security)

Briefly describe the basic measures in the data protection concept. For technical details provide a separate IT security concept.

- How is the network communication protected?
- How is the protection of the network regulated on the physical, logical and application level (e.g. spatial separation of server infrastructures, firewalls, routing, IP filters, and authentication)?
- Who has access to the project network?
- How are servers protected against attacks from outside / unauthorized access (in particular describe server hardening[25])?
- How is security provided for end users (especially necessary local security measures for client computers and other end devices) and which prerequisites must be fulfilled to establish a network connection to the project databases?
- How are certificates distributed and used?
- Are virtualisation techniques used?
- Are relevant parts of the BSI IT Basic Protection catalogues[26] taken into account (e.g. access controls, data carrier controls)?

[25] Technical term that describes how far servers are immune to attacks from the network.

F. Backup strategy

- How and how often is data backed up?
- How is backed up data protected?
- Are backups encrypted? If yes, who has the backup data? Who has a copy of the backup data? Where is backup data stored in case of emergency? Who is responsible for encryption? How is the backup data encrypted in detail? How does encryption influence automatic data backup?
- How is the data protected from unauthorized access?
- How is the data protected from accidental / deliberate modification / deletion?
- Who has access to the data backups?
- How is data deleted from the backup files?
- Are there redundant systems in case of a system failure?

G. Used encryption technology

The encryption methods used and their integration shall be described.

- Which encryption technology is used to secure the communication connections?
- Which encryption technology is used to secure the data memory?
- Which encryption technology is used for pseudonymisation procedures?

H. Pseudonymisation

The technical implementation aspects of the pseudonymisation procedures shall be presented.

- Are test persons assigned unique identifiers in the form of pseudonyms?
- If so, which technical procedures form the basis of this assignment?
- How does a depseudonymisation (resolution of a pseudonym) take place?
- If different pseudonyms are used in different modules: How is the assignment done?
- Is the use of record linkage methods planned?
- If the pseudonymisation procedure has to be changed: How is the re-pseudonymisation carried out?

I. Failure protection

- What effects can a system failure have on project operation?
- Which measures can be taken against it?

[26] See references

VII. The "commandments" of data protection laws on IT security

Have the requirements of data protection laws on IT security been sufficiently taken into account? Note: The security of the processing of personal data with respect to the state of the art, the implementation costs and the type, the scope, circumstances and purposes, as well as the different probabilities of occurrence and the severity of the risk to rights and freedoms is a core element of the GDPR[27]. Accordingly, appropriate technical and organisational measures should be put in place to ensure a level of protection appropriate to the risk in order to pseudonymise and encrypt personal data, the ability to ensure the long-term confidentiality, integrity, availability and resilience of systems and services related to the processing, and the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident.

Comparison with the TMF Data Protection Guideline

Deviations from the Data Protection Guideline should be summarized and justified. This serves to facilitate assessment by the TMF and by data protection officers.

- On what points are deviations from the guideline necessary?
- What proportionality[28] considerations[29] underlie the deviations?

[27] Art. 32 GDPR

[28] Some common simplified architectural variants are defined in the appendix to the generic data protection concept for biomaterials banks (see preamble).

[29] Some frequently occurring simplified architecture variants are listed in the appendix of the generic data protection concept for biomaterial banks (see preamble).

Glossary

This glossary is based on definitions from the TMF's Guide to the development of a data protection concept for a medical research project.

Annotation (data)

Medical data (MDAT) containing the diagnostic and therapeutic information associated with a sample. They are to be distinguished from purely administrative data, which represent non-personal technical and organizational information about a sample.

Anonymisation

Anonymisation is the abolition of the personal relationship of data to a person. "Anonymisation is the alteration of personal data in such a way that the individual details of personal or factual circumstances can no longer be attributed to a specific or identifiable natural person, or can only be attributed with a disproportionately large expenditure of time, money and labour.

Archiving

Permanent storage of data on suitable data carriers

Audit

An audit is generally defined as an examination procedure used to evaluate processes with regard to the fulfilment of requirements and guidelines.

Clarification

See Patient Information

Confidentiality

Medical secrecy is the ethical and legal duty of the physician to maintain secrecy about everything that becomes known to him about a patient in the exercise of his profession (protection of patient secrecy).

BDSG

Federal Data Protection Act

Biobank (biomaterial bank, sample bank, tissue bank, gene bank, sample collection)

A biobank is a facility which collects samples of human bodily substances, prepares them where appropriate, supplements them with demographic and disease-related ("medical") data of the subject and makes samples and data available in an appropriate form for research purposes.

Biomaterial

See sample

Data trustee

See Trustee

Depseudonymisation

Authorised restoration of the personal reference of pseudonymised data and samples

Declaration of consent (informed consent, consent after clarification and declaration of consent)

The condition required by data protection law for the processing of personal data of the data subject, unless this is permitted by law.

GDPR

General Data Protection Regulation

IDAT = Personal or identifying data

Personal data "means any information relating to an identified or identifiable natural person; 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 one or more particular characteristics which are an expression of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person[30]

MDAT = research data or medical data

MDAT is the umbrella term for data stored for research purposes in the central database of a medical research network. MDAT usually comprises clinical facts such as findings and diagnoses as well as sociodemographic data that allow the patient or volunteer to be classified for scientific purposes.

Monitor (clinical monitor)

The clinical monitor monitors clinical trials, in particular in accordance with the Medicines Act.

Patient

see test person

Patient information

Notification to the participant of a research project what will happen to his data and, if applicable, samples.

Pseudonymisation

pseudonymisation" means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the provision of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures ensuring that the personal data are not attributed to an identified or identifiable natural person[31]

PSN = Pseudonym

The PSN is a non-speaking identifier of a patient or subject (letters or numbers that do not indicate the personal identifying data).

Re-identification

By means of re-identification, the personal reference of anonymised or pseudonymised data and samples is restored without authorization.

Test persons

[30] cf. Art. 3 para. 1 GDPR 2016/679

[31] cf. Art. 3 para. 5 GDPR 2016/679

Patient and volunteer are the persons who provide the research network with data on their health and materials of their body for biomedical research purposes. If the data collection or sampling takes place in the context of treatment, the donor is the "patient". If the data collection or sampling takes place in the research context, the donor is "subject". The term "subject" is also used as a generic term for "patient and/or subject", especially if a control group is involved in the study.

TMF

technology and method platform for networked medical research e.V.

Trustee

The data trustee is a legally, spatially and personnelally independent, who is ideally subject to a special confidentiality obligation, e.g. a notary or an external doctor.

Rehearsal

Substance removed from the human body for diagnostic or scientific purposes

Withdrawl

The revocation of the use of data or samples means the partial or complete withdrawal of the declaration of consent (see there) with the consequence that data (data categories) and samples from the research association may not be used, or only to a limited extent, for own or third-party research projects. After the revocation of the declaration of consent, the agreement with the patient or subject may also include the obligation to delete or anonymise data or to hand over the sample to the subject, to destroy it or at least to make it anonymous. It is also conceivable that the declaration of consent may not be revoked.

References

[I] Data protection concept template of the *MOSAIC project* (*Institute for Community Medicine, University Greifswald ICM*)
https://mosaic-greifswald.de/werkzeuge-und-vorlagen/datenschutzkonzept.html

[II] Guideline for create data protection concepts in health care (*German society for medical informatics, biometry and epidemiology GMDS*)
https://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

[III] Standard data protection model (SDM, *92th Conference of independent data protection authorities of Germany*)
https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf

[IV] Actual recommendations for data protection of research data (*Council for information infrastructures RFII*, 2017)
http://www.rfii.de/de/category/dokumente/

[V] Actual demands of the German Data Protection Act (BDSG)
https://www.gesetze-im-internet.de/bdsg_1990/index.html#BJNR029550990BJNE001902301

[VI] European General Data Protection Regulation (EU-GDPR 2016/679)
https://gdpr-info.eu/