LAW & INNOVATION

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

JÖRG POHLE, NILS HEINEMANN, MAXIMILIAN VON GRAFENSTEIN, VALENTIN RUPP

Certification program for processing personal data in the context of data sharing in the health & care sector

HIIG DISCUSSION PAPER SERIES 2026-03

ABSTRACT

The present conformity assessment program was developed within the framework of the BMFTR-funded project "ProKIP: Prozessentwicklung und -begleitung zum KI-Einsatz in der Pflege" (Process development and support for the use of AI in nursing). ProKIP supported, advised, connected, and evaluated research projects within the BMFTR funding program "Making Repositories and AI Systems Usable in Everyday Nursing Practice."

Based on the findings of the project, this conformity assessment program was designed and developed. It serves as a preliminary stage for a data protection certificate pursuant to Article 42 GDPR and ensures the GDPR-compliant and thus legally safe application of the project results in nursing practice.

The program covers the processing of personal data from healthcare and nursing institutions for the purpose of transmitting, disseminating or otherwise making available ("sharing") (or preparing and preprocessing to share) either data-minimised or fully anonymised health or care data to third parties for downstream purposes. The scheme distinguishes two options that can be chosen by the scheme applicant, one with higher requirements for the preprocessing, and one with higher requirements for the disclosure of the preprocessed data: (1) When the scheme applicant chooses the first option, the preprocessing of the data entails data minimisation procedures which do not guarantee full anonymisation. The scheme applicant then has to fulfil higher requirements in order to be permitted to disclose the data to third parties, as put down in this scheme. (2) When the scheme applicant chooses the second option, the preprocessing of the data entails full anonymisation, which has to be demonstrated by the scheme applicant. The scheme applicant then has to fulfil lower requirements in order to be permitted to disclose the data to third parties, as put down in this scheme.

The program specifies the necessary protective measures, as well as the type and form of the evidence to be provided and the methods for verifying such evidence.

KEYWORDS

AI in Care, Health data, Pseudonymisation, Anonymisation, Synthetisation, Data sharing, Data protection, GDPR, Conformity assessment program, Certification program

CITATION

Pohle, J., Heinemann, N., Grafenstein, M. v., & Rupp, V. (2026). Certification program for processing personal data in the context of data sharing in the health & care sector. HIIG Discussion Paper Series 2026-03. 67 pages. https://doi.org/10.5281/zenodo.18455303.

AUTHOR INFO / AFFILIATION / FUNDING

Dr. Jörg Pohle, Alexander von Humboldt Institute for Internet and Society, Berlin.

Nils Heinemann, Alexander von Humboldt Institute for Internet and Society, Berlin.

Prof. Dr. Max von Grafenstein, LL.M., Alexander von Humboldt Institute for Internet and Society, Berlin; Law & Innovation Technology GmbH, Berlin.

Valentin Rupp, Law & Innovation Technology GmbH, Berlin.

The project was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) under grant no. 16SV8858.

VERSION HISTORY

Version number	Date of completion	Adapted by
0.9	20 May 2025	Nils Heinemann, Jörg Pohle
1.0	7 August 2025	Valentin Rupp, Max von Grafenstein, Jörg Pohle

CONTENT OVERVIEW

TABLE OF CONTENTS

I. SCOPE

1. Scheme applicant (SA)

The scheme applicant (SA) is either (1) a health or care institution, or (2) an individual or consortium-based project in the health and care sector, with the objective of sharing (or preparing and preprocessing to share) either (a) data-minimised or (b) fully anonymised health or care data with third parties.

2. Target of Evaluation (ToE)

In order to facilitate the certification of SA and make the conformity assessment more cost-efficient, this certification scheme limits its scope in multiple ways.

2.1 Purpose and processing operations

The ToE includes only processing operations conducted by the SA for the following purpose:

> **Health and treatment data originating from a clinical institution are to be data-minimised or fully anonymised to allow for disclosure by transmission, dissemination or otherwise making available ("sharing") to third parties for downstream purposes.**

The scheme distinguishes two options that can be chosen by the SA, one with higher requirements for the preprocessing, and one with higher requirements for the disclosure of the preprocessed data:

(a) When the SA chooses the first option, the preprocessing of the data entails data minimisation procedures which do not guarantee full anonymisation. The SA then has to fulfil higher requirements in order to be permitted to disclose the data to third parties, as put down in this scheme.

(b) When the SA chooses the second option, the preprocessing of the data entails full anonymisation, which has to be demonstrated by the SA. The SA then has to fulfil lower requirements in order to be permitted to disclose the data to third parties, as put down in this scheme.

2.1.1 Data subjects

Data subjects are the patients of the clinical or care institutions whose personal data are included in the datasets that are to be data-minimised or fully anonymised in order then to be disclosed, i.e. in data-minimised or anonymised form, to third parties.

2.1.2 Other actors

'Platform' means any intermediation service as referred to in Article 2, point (11), of Regulation (EU) 2022/868, the Data Governance Act, including one that aims to establish non-commercial relationships for the purpose of data sharing as referred to in Article 2, point (10), of Regulation (EU) 2022/868.

'Data recipient' means a natural or legal person to whom the SA makes data-minimised or fully anonymised data available through a platform for further use.

2.1.3 Risks

Human dignity (Art. 1 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection of human dignity under Article 1(1) of the German Basic Law (GG) and Article 1 of the EU Charter of Fundamental Rights (EU-CFR).

Integrity of the person (Art. 3 EU-CFR)

The future processing and use (or re-use) for downstream purposes entails risks to the data subjects' fundamental right to bodily integrity under Article 2(2) of the German Basic Law (GG) and Article 3 of the EU Charter of Fundamental Rights (EU-CFR).

Private and family life (Art. 7 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection of private and family life under Article 2(1) in connection with Article 1(1) as well as Article 6 of the German Basic Law (GG) and Article 7 of the EU Charter of Fundamental Rights (EU-CFR).

Data protection (Art. 8 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to informational self-determination under Article 2(1) in connection with Article 1(1) of the German Basic Law (GG) and the protection of personal data under Article 8 of the EU Charter of Fundamental Rights (EU-CFR).

Non-discrimination (Art. 21 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection from discrimination under Article 3 of the German Basic Law (GG) and Article 21 of the EU Charter of Fundamental Rights (EU-CFR).

Equality between women and men (Art. 23 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection of equality between women and men under Article 23 of the EU Charter of Fundamental Rights (EU-CFR).

Rights of the child (Art. 24 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection of the rights of the child under Article 24 of the EU Charter of Fundamental Rights (EU-CFR).

Rights of the elderly (Art. 25 EU-CFR)

The data minimisation or anonymisation process preceding the disclosure, the disclosure of minimised data as well as the future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to the protection of the rights of elderly under Article 25 of the EU Charter of Fundamental Rights (EU-CFR).

Social security and social assistance (Art. 34 EU-CFR)

The future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to social security and social assistance under Article 34 of the EU Charter of Fundamental Rights (EU-CFR).

Health care (Art. 35 EU-CFR)

The future processing and use (or re-use) for downstream purposes entail risks to the data subjects' fundamental right to health care under Article 35 of the EU Charter of Fundamental Rights (EU-CFR).

Further risks to fundamental rights

Next to these mentioned risks, the future processing and use (or re-use) for downstream purposes may lead to further, yet undetermined risks to fundamental rights and freedoms, depending on the context, the social actors involved, the purposes as well as the means employed.

2.1.4 Benefits

Due to the technically and legally complex access to health and treatment data, the potential for using or re-using the health and care data for downstream purposes has not yet been fully realised.

The implementation of appropriate data-minimisation or anonymisation procedures prior to disclosing the data to third parties enables the data protection-compliant use and re-use of health and treatment data. In particular, it allows for improvement of health and care, knowledge gain in health and care research, further development of AI technologies and more.

2.2 No data transfer under option (a)

Transfer of personal data, i.e. data minimised according to option (a), to third countries according to Articles 44 ff. GDPR is not admissible under this scheme.

2.3 Higher requirements for some criteria

The scheme facilitates the assessment of GDPR conformity in some cases by defining requirements that go beyond those imposed by the GDPR. This applies in particular to the (unrestricted) obligations to appoint a DPO and carry out a risk assessment that fulfils the requirements of a data protection impact assessment pursuant to Article 35 GDPR, to maintain a documentation of the data minimisation or anonymisation specification, implementation, execution and testing, and to fulfil additional duties when selecting a data sharing platform.

The scheme includes the following provisions that go beyond the legal requirements of the GDPR:

1. Notwithstanding the limits of the respective provision in the GDPR or any national data

protection regulation, a DPO has to be appointed.

2. A data protection impact assessment (DPIA) pursuant to Article 35 GDPR must be carried out and documented.

3. A documentation of the data minimisation or anonymisation specification, implementation, execution and testing must be maintained that goes beyond the requirements of the GDPR.

4. The SA has to fulfil duties when selecting a data sharing platform that go beyond the requirements of the GDPR and encompass duties that concern the sharing of anonymised data.

5. The SA has to engage platforms for making data available to third parties, which have to fulfil requirements that go beyond those imposed by the GDPR and have to be able to demonstrate that their disclosure is performed in accordance with this scheme.

3. Territorial Scope

The certification scheme is directed towards:

- SA based in EEA Member States

The scheme is not to be used as a tool for transfers (Article 46 GDPR) for entities in third countries that are not subject to the GDPR.

II. CRITERIA CATALOGUE

This criteria catalogue for processing personal data in the context of data sharing in the health & care sector contains the following criteria:

1. Data protection officer (DPO)
2. Documentation
3. Definition of roles and responsibilities (controllers and processors)
4. Purpose specification and limitation with respect to its processing operation
5. Data protection (risk and) impact assessment
6. Legal base according to the GDPR
7. Data minimisation
8. Rule setting, binding and enforcement
9. Identifiability of the data recipient
10. Purpose specification and limitation with respect to the data re-use
11. Information to data recipients
12. No linking
13. Population and purpose compatibility
14. Data protection by design

15. Re-Identification prohibition
16. Transparency
17. Data subject rights
18. Storage limitation
19. Third country transfer
20. Data breach
21. IT-Security

Colour coding:

Application criteria
Specific criteria
General criteria

1. Data protection officer (DPO)

Requirement in a nutshell:
The SA designates a data protection officer (DPO) according to Art. 37 GDPR.

Relevant norms:
Art. 37, Art. 38, Art. 39, Art. 27, Art. 12 (1), 13 (1)(b), Art. 24, Art. 31 GDPR **Application criteria**

1.1 Formal designation of a DPO

The SA has designated a DPO (irrespective of the SA's size, legal structure or core activities), formally addressing the following tasks and duties to the DPO pursuant to Article 39(1) GDPR in a manner compliant with Article 39(2) GDPR:

- to provide advice to the SA and its personnel with regard to all questions concerning the compliance to duties imposed by the GDPR, including the performance of an impact assessment according to Article 35 GDPR,
- to monitor compliance of the SA and its personnel with the GDPR,
- to cooperate with and to act as the contact point for the supervisory authority and the CAB.

If the SA is a consortium-based project, the designated DPO may be the DPO of one of the consortium partners.

1.2 Attributes of the DPO

The SA has implemented processes to assess and ensure the DPO (Article 37(5) GDPR):

- has expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR;[1]
- has some general knowledge of the health and care sector,
- has sufficient understanding and overview of the processing operations performed according to this scheme and the information systems to facilitate these processing operations,[2]
- is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38 (5) GDPR)
- does not perform tasks and duties that create an obvious conflict of interests (Article 38 (6) GDPR)
- is physically based in the EU: If the DPO is based outside the EU the SA has assessed why the DPO can perform its duties equally or more effectively outside the EU (e.g. because the company itself is located outside of the EU).[3]

1.3 Independence

The SA has implemented processes to ensure the independence of its DPO (Article 38 (3) GDPR) by:[4]

- ensuring the DPO does not receive any instructions regarding the exercise of its tasks and duties as DPO,
- ensuring the DPOs contract is not cancelled, its chances for promotion and its chances to receive bonuses as well as the DPOs work in general are not affected as a consequence of its work as DPO. This does not affect the SAs ability to sanction the DPO for actions unconnected

[1] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 11.
[2] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 11.
[3] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 11.
[4] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 12.

to its role as DPO (e.g., theft, physical, psychological or sexual harassment or similar gross misconduct),[5]
- if the DPO is not part of the organisation of the SA (Article 37(6) GDPR), inhibiting unfair termination of service contracts for activities as DPO and inhibiting unfair dismissals of any individual member of the organisation carrying out DPO tasks.

1.4 Tasks of the DPO

The SA has implemented processes to assess and ensure the DPO conducts the following tasks and duties pursuant to Article 39(1) GDPR in a manner compliant with Article 39(2) GDPR:
- inform and advise the SA and all its personnel involved in sharing health or care data with third parties regarding their obligations under the GDPR,
- monitor compliance with the GDPR and other data protection regulations, as well as the strategies of the SA for protecting personal data, including the assignment of responsibilities, awareness raising, and training of all personnel involved in sharing health or care data with third parties, and conducting related reviews,
- provide advice in connection with the data protection impact assessment (DPIA) pursuant to Article 35 GDPR and monitoring its mandatory execution,
- cooperate with the supervisory authority
- serve as the point of contact for the supervisory authority in matters related to the processing involved in sharing health or care data with third parties.

1.5 Support of the DPO

The SA has implemented processes to assess the appropriate time within which the DPO should process and respond to requests and the necessary means to enable the DPO to apply to this timeframe.

The SA has implemented processes to assure the DPO is provided with sufficient resources to effectively exercise its duties accordingly (Article 38(2) GDPR). This includes[6]:
- adequate financial resources,
- infrastructure (premises, facilities, equipment),
- contact with project partners and individual consortium partners, if applicable,
- access to key stakeholders (e.g. care professionals, patients) in order to make the necessary assessments,
- continuous training, to stay up to date with the state of the art and legal requirements concerning questions addressed in any criteria within this scheme.

The SA has implemented processes to:
- involve the DPO in a timely manner with all issues relating to the protection of personal data (Article 38(1) GDPR),
- grant access to the highest management level to the DPO in case it identifies incompatibilities with the GDPR (Articles 38(1), 38(3)(3) GDPR)
- and take into account the DPO's opinion regarding each criteria imposed by this certification scheme.

1.6 Data protection by design

The SA has implemented effective measures to ensure the DPO aligns with these requirements and is

[5] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 16.
[6] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 14.

easily and directly accessible to data subjects, supervisory authorities, the CAB and departments within the SA and is able to receive, process and respond to requests within an appropriate time frame (Article 38(4) GDPR).

Proof / Evidence	Assessment methods
• Internal DPO concept (including task & process descriptions, policies, organizational charts) • DPO contract and certificate of appointment (If the SA is a consortium-based project, the contract may be closed between the DPO and one of the consortium partners) • Evidence of the DPO's qualification (such as degrees, certificates) • Reporting the contact details of the DPO to the competent supervisory authority • Presentation of the DPO as a contact person on the SA's website • Proof of hours worked	• Formal document check • Legal review (to clarify unclear terms) • Internal audit records as evidence of activities, independence, as well as the involvement and effectiveness of the DPO • Interview with the DPO regarding their tasks as evidence of the absence of a conflict of interest

1.7 Transparency

The SA publishes the contact details of the DPO and communicates them to data subjects, relevant supervisory authorities, the CAB and the staff within the SA[7] and (Article 37(7) GDPR), making accessible at least one of the following information:

- a postal address,
- a dedicated telephone number,
- a dedicated email address.

(Article 37(7) GDPR does not require the contact details to include the name of the DPO.[8])

Proof / Evidence	Assessment methods
• Data protection policy • Reporting the contact details of the DPO to the competent supervisory authority • Presentation of the DPO as a contact person on the SA's website	• Formal document check • Legal review (to clarify unclear terms)

1.8 Documentation

The SA has implemented measures to document:

- the assessment of an appropriate response time,
- the assessment to determine necessary means provided to the DPO, and
- the assessment whether a DPO which is based outside the EU can exercise its duties equally or more effectively outside the EU.

The SA has implemented measures to document the reasons whenever they do not act in accordance

[7] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 14.
[8] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 13.

with the DPO's advice concerning any question imposed by this certification scheme.[9]

Proof / Evidence	Assessment methods
• DPO contract • Internal DPO concept (including task & process descriptions, policies, organizational charts, resources) • Disagreement / deviation case documentation with justifications	• Formal document check • Legal review (to clarify unclear terms)

1.9 Monitoring

The SA monitors whether the response time remains appropriate and whether the DPO applies to this timeframe.

In case a single DPO is made responsible for several or all bodies within a group of undertakings, the SA monitors whether the DPO is able to perform all tasks efficiently.[10]

Proof / Evidence	Assessment methods
• Eventually updated DPO contract and internal DPO concept[11] • Random sample after 1 year	• Formal document check and legal review (to clarify unclear terms) • Audit (org): Interview with DPO

[9] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 14.
[10] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 10.
[11] The certification contract between the SA and CAB contains an obligation for the SA to notify the CAB of any changes made concerning the relationship to the DPO.

2. Documentation (esp. Art. 30 and 35 GDPR)

Requirement in a nutshell:
The SA fulfils all documentation requirements.

Relevant norms:
Art. 30, Art. 5 (2), Art. 24 (1), Art. 7 (1), Art. 12 (1), Art. 25 (1), Art. 26 (1), (2), Art. 28 (3), (4), (9), Art. 33 (5), 35 GDPR **Application criteria**

2.1 Record of processing activities

The SA maintains a record of processing activities (this requirement applies also in case the SA fulfils any exemptions according to Article 30(5) GDPR) that contains the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the representative of the controller, and any data protection officer;
- the purpose and sub-purposes of the processing;
- a description of the categories of data subjects and the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or to an international organization, including the identification of the third country or international organization involved, and, in the case of transfers referred to in Article 49(1) second subparagraph of the GDPR, documentation of appropriate safeguards;
- the intended time limits for erasure of the different categories of data;
- a general description of the technical and organizational measures pursuant to Article 32(1) GDPR.

The SA maintains a record of the following information, which goes beyond the requirements of Article 30(1) GDPR, but is substantively necessary and associated with a data protection impact assessment (DPIA):

- a description of other involved actors;
- a description of the roles and legal relationships between the actors;
- a description of the processing activities of the use cases, as well as the nature of the technical systems and services used, including software and interfaces;
- the legal basis for the processing activities;
- a data protection risk analysis with links to the respective parts of the DPIA.

2.2 Data minimisation or anonymisation process and outcome

The SA maintains documentation concerning the data minimisation or anonymisation process and outcome. The documentation covers the following:

- an initial data assessment report;
- a data minimisation or anonymisation concept;
- a data minimisation or anonymisation report;
- a data quality and minimisation / anonymity assessment concept;
- a data quality and minimisation / anonymity assessment report.

The SA ensures that the **initial data assessment report** contains an evaluation of the data concerning:

- the data's quality, i.e., the degrees of adequacy and relevance in relation to foreseeable downstream purposes for which they might be processed, the completeness and accuracy,

- the population that is represented in the data, including their statistical characteristics, as well as possible edge cases, fairness issues etc., and,
- if applicable and necessary for understanding and (re-)using the data, the means by which the data has been collected or generated.

The SA ensures that the **data minimisation or anonymisation concept** contains:
- a description of the data that is to be minimised or anonymised,
- the specification of roles and responsibilities for the data minimisation or anonymisation,
- the data minimisation or anonymisation methods to be used, and
- the way in which the data minimisation or anonymisation will be documented.

The SA ensures that the **data minimisation or anonymisation report** contains:
- information concerning the persons who carried out the data minimisation or anonymisation process,
- information concerning the steps taken according to the specified methods as well as their order,
- information concerning the data and time when the data minimisation or anonymisation was carried out and completed, and
- information concerning the outcome of the data minimisation or anonymisation process.

The SA ensures that the **data quality and minimisation / anonymity assessment concept** contains:
- the specification of roles and responsibilities for the data quality and minimisation / anonymity assessment,
- the specification of the (possible downstream) purposes for which the data quality will be assessed,
- the data quality and minimisation / anonymity assessment methods to be used, and
- the metrics and/or threshold values that will be used to assess the quality of the data as well as the quality of the achieved data minimisation or anonymisation, and
- the way in which the data quality and minimisation / anonymity assessment will be documented.

The SA ensures that the **data quality and minimisation / anonymity assessment report** contains:
- information concerning the persons who carried out the data quality and minimisation / anonymity assessment,
- information concerning the steps taken according to the specified methods as well as their order,
- information concerning the data and time when the data quality and minimisation / anonymity assessment was carried out and completed,
- information concerning the outcome of the data quality and minimisation / anonymity assessment, and
- proofs that the outcome of the data quality and minimisation / anonymity assessment meets the specified criteria.

2.3 Data disclosure

The SA maintains documentation concerning the data disclosure that contains the following:
- a data disclosure concept;
- a market survey with service specifications / descriptions of the platforms that are taken into consideration in the selection process;
- a platform selection and reasoning document;
- a contract with the platform selected concerning the data disclosure.

2.4 Data protection by design

The SA has implemented measures to structure the documentation in a clear and understandable way.[12]

The SA has implemented measures to separate the documentation from other documentation conducted in compliance with other regulation, which is not subject to this scheme (e.g. tax audits).[13]

Proof / Evidence	Assessment methods
• Record of processing activities • Data minimisation or anonymisation process, outcome and assessment documentation • The entirety of documented compliance to data protection regulation as defined in 2.1	• Formal document check and legal review (to clarify unclear terms) • Audit (org): interview with DPO

2.5 Monitoring

The SA has implemented processes to keep the documentation up to date.

The SA archives old versions and attributes to each version:[14]

- a versioning number,
- date and time when the documentation was last updated,
- by whom the documentation was last updated.

Proof / Evidence	Assessment methods
• Eventually updated documentation[15] • Random sample after 1 year wrt processes • Time stamps • Version history	• Formal document check and legal review (to clarify unclear terms) • Audit (org): interviews with employees

2.6 Data Protection Impact Assessment documentation

The SA maintains a documentation of the data protection impact assessments according to Article 35 GDPR.

Proof / Evidence	Assessment methods
• Documentation of data protection impact assessments • Random sample	• Formal document check and legal review (to clarify unclear terms) • Audit (org): Interview with DPO

[12] See DSK, SDM Baustein 42 „Dokumentieren", Version V1.0a, M42.P01.
[13] See DSK, SDM Baustein 42 „Dokumentieren", Version V1.0a, page 2.
[14] See DSK, SDM Baustein 42 „Dokumentieren", Version V1.0a, page 3.
[15] The certification contract between the SA and CAB contains an obligation for the SA to notify the CAB of all changes to the documentation.

3. Definition of roles and responsibilities (controllers and processors)

Requirement in a nutshell:
The SA correctly attributes responsibility to itself and all data receivers as data controller, processor and/or joint controller.

Relevant norms:
Art. 4 (7), (8), (9), (10), Art. 5 (1)(a),(b),(c),(f), Art. 13 (1)(e), Art. 25 (1), Art. 29, Art. 30 (1)(d) GDPR

Application criteria

The SA correctly recognises all relevant actors related to the processing activity or activities.

The SA maintains an up-to-date record of all relevant actors, their roles and responsibilities.

3.1 Specification of the SA's own role as data controller

The SA correctly recognises itself as a data controller, either as a sole controller or as a joint controller.

If the SA recognises itself as a joint controller, it also correctly recognises all other bodies that are part of this joint controllership.

3.2 Clarification of the role of all data recipients

The SA correctly recognises all recipients in their respective roles with regards to the processing activities. For this purpose, the SA has implemented processes to assess whether any processing operation includes the transfer of personal data either to an internal or an external entity (esp. companies), which:

- are authorised to process the data under the direct authority of the controller (internal data receiver – see Art. 4 (10) GDPR)
- process the data on behalf of the scheme applicant (processor Art. 4 (8) GDPR)
- jointly decide with the website provider on the purposes and means of the processing of data (joint controller Art. 4 (7) GDPR)
- or none of the above (third party = separate controller) Art. 4 (10) GDPR.

3.3 Data protection by design

The scheme applicant has implemented effective measures to ensure that personal data is only transmitted to internal data receivers and processors and joint controllers conforming to the requirements described in II.3.7. and II.3.8, and to stop all processing of personal data related to entities not conforming to these requirements = "third party" data receivers acc. to Art. 4 (10) GDPR.

Proof / Evidence	Assessment methods
• Record of processing activities • Data Processing Agreement • Joint Controller Agreement • On request: access to IT-System (e.g. cookiescan – see list below: How to demonstrate compliance to the CAB)	• Formal document check • Audit (org): Interview with DPO • Technical inspection (e.g. by conducting a cookiescan)

3.4 Transparency

The scheme applicant has implemented effective measures to inform the data subjects about all data

receivers (see II.16. Transparency).

Proof / Evidence	Assessment methods
• Cookie banner or other consent form • Privacy policy	• Formal document check

3.5 Documentation

The scheme applicant has implemented effective measures to document all data receivers and their roles according to II.3.2 (see also II.2. Documentation).

Proof / Evidence	Assessment methods
• Record of processing activities • Documented data protection risk and impact assessment (DPIA) • Data Processing Agreements • Joint Controller Agreements	• Formal document check • Review (to clarify unclear terms)

3.6 Monitoring

The scheme applicant checks on a regular basis, whether it has correctly specified all data receivers and whether the conduct of these data receivers has changed in a way that impacts the definition of their roles and responsibilities according to II.3.2.

Proof / Evidence	Assessment methods
• Eventually updated documentation[16] • Random sample within one year of certification wrt checks	• Formal document check and review (to clarify unclear terms) • Audit (org): Interview with DPO

3.7 Criteria concerning the use of processors

Requirement in a nutshell:
The SA enters into a data processing agreement with all parties which process personal data on behalf of the SA (i.e. data processors).

Relevant legal norms:
Art. 28, Art. 4 (7), (8), (9), Art. 13 (1)(e), Art. 25 (1), Art. 30 (2), Art. 32, Art. 33-36 GDPR

Application criteria

The SA enters into a data processing agreement with all parties which process personal data on behalf of the SA (i.e. data processors) for the purpose and sub-purposes within the given scope of this scheme (as defined in chapter I).

The SA ensures that the engagement of a data processor meets the following requirements set out in

[16] The certification contract between the scheme applicant and CAB contains an obligation for the scheme applicant to notify the CAB of all changes to the documentation.

Article 28 of the GDPR:

3.7.1 Valid processing agreements

The scheme applicant enters with all processors into a valid data processing agreement, conforming to the following requirements:

3.7.1.1 Valid written or electronic DPA (Art. 28 (9) GDPR)

The DPA is issued in written or electronic form. All essential requirements for the validity of the contract are met. In particular, the written or electronic signature by a natural person who is authorised to represent the company is given.

3.7.1.2 The DPA contains all generally required terms

3.7.1.2.1 Information about contracting parties[17]

The contract includes at least the following information about the scheme applicant and the processor:

- name,
- address,
- name, function and contact details of the contact person of each party,
- if applicable, information regarding the data protection officer of each party
- If applicable, the representative

3.7.1.2.2 Categories of the personal data (Art. 28 (3)(1) GDPR)

The DPA lists all categories of personal data processed by the processor on behalf of the scheme applicant. (see II.4. Purpose specification and limitation with respect to its processing operation)

3.7.1.2.3 Source of the data and client separation

The DPA obligates the processor to only process personal data received by the scheme applicant or collected otherwise as instructed by the scheme applicant.

The DPA obligates the processor not to store or otherwise process this personal data together with other personal data (e.g. the data received from other scheme applicants), unless the scheme applicant specifically instructs the processor to do so.

3.7.1.2.4 Categories of data subjects (Art. 28 (3)(1) GDPR)

The DPA specifies the categories of data subjects in accordance with the I. Scope.

3.7.1.2.5 Purpose specification (Art. 28 (3)(1) GDPR)

The DPA lists all processing purposes for which the processor is being instructed to perform data processing operations on behalf of the scheme applicant.

3.7.1.2.6 Purpose limitation (Art. 28 (3)(1) in conjunction with Art. 28 (3)(2)(a), Art. 29 GDPR)

The DPA obligates the processor:

- to process personal data only for the purposes determined by the scheme applicant
- to process only the categories of personal data requested by the scheme applicant
- to generally limit the processing operations to the instructions received from the scheme applicant

[17] See European Commission, Annex I List of Parties of the Annex to the Commission implementing decision on standard contractual clauses between controllers and processors, C(2021) 3701 final, 4.6.2021.

- to store the personal data only for the duration necessary to provide the service, at most for as long as determined by the scheme applicant.

3.7.1.2.7 Storage duration (Art. 28 (3)(1), Art. 28 (3)(2)(g) GDPR)

The DPA assigns to the scheme applicant the unconditional right to at any time instruct the processor to

- stop the processing of personal data
- delete the personal data
- return the personal data,

unless Union or Member State law requires the scheme applicant to store the personal data.

The DPA at least conclusively determines a maximum duration for which the processor is allowed to store and otherwise process personal data.

3.7.1.2.8 Confidentiality and security of processing (Art. 28 (3)(2)(b) and (c), Art. 32 GDPR)

The DPA requires the processor to specify and implement appropriate technical and organisational measures acc. to Art. 32 GDPR.

The DPA requires the processor to ensure that persons authorised to process the personal data have contractually committed themselves to confidentiality or already are under an appropriate statutory obligation of confidentiality.

3.7.1.2.9 Sufficient guarantees (Art. 25, Art. 28 (1) GDPR)

The DPA obligates the processor to implement sufficient technical and organisational measures to comply with all requirements imposed by the DPA and/or the GDPR.

3.7.1.2.10 Support of the scheme applicant to ensure compliance with GDPR requirements (Art. 28 (3)(2)(a),(e),(f),(h), Art. 33 – 36 GDPR)

The DPA obligates the processor within its means to assist the scheme applicant:

- in fulfilling its duties to respond to requests for exercising the data subject's rights (lit. e)
- in ensuring compliance with the process for reporting data breaches acc. to Art. 33 and 34 GDPR, e.g. by description of used data, processing operations and technical and organisational measures (lit. f) and
- in conducting a data protection impact assessment acc. to Art. 35 GDPR and prior consultation of the data protection authorities acc. to Art. 36 GDPR (lit. f).

The DPA obligates the processor to notify the scheme applicant of any processing operations to which the processor is required by law before conducting these processing operations, unless the law in question prohibits such notification on grounds of important public interest (lit a).

The DPA obligates the processor to make available to the controller all information necessary to demonstrate compliance with the DPA and to contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (lit. h). This also includes proof of the processor's cooperation with supervisory authorities (Art. 31 GDPR).

3.7.1.2.11 Maintaining a record of processing activities (Art. 30 (2) GDPR)

The DPA obligates the processor to document in a record of processing activities all categories of processing activities carried out on behalf of a scheme applicant, containing the following information:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's

representative, and the data protection officer,
- the categories of processing carried out on behalf of each controller,
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation,
- where possible, a general description of the technical and organisational security measures referred to in Art. 32 (1) GDPR.

3.7.1.2.12 Subprocessors (Art. 28 (2) GDPR)

The DPA requires the processor to not engage other processors for carrying out specific processing activities on behalf of the controller (sub processors), before receiving from the scheme applicant in written (or electronic) form either:

- **Specific authorisation:**
  In a specific authorisation the scheme applicant has to specify which subprocessor and what processing activity it refers to specifically. Any subsequent change in this case will need to be further authorised by the controller before it is put in place.[18]
- **Or general authorisation:**
  For a general authorisation the scheme applicant generally allows the use of subprocessors for certain processing operations by providing a list with such sub-processors in an annex thereto.[19]

The DPA requires the processor in the case of general authorisation to inform the scheme applicant immediately of any intended change with regard to the involvement or replacement of other (sub)processors, including details of the name, address and the specific processing activity of the subprocessor. The DPA also grants the right to object to such changes within a reasonable time period defined in the DPA, with the consequence that the processing activity of the (sub)processor involved must cease immediately (Art. 28 (2)(2) GDPR).

The DPA obligates the processor in the case of using sub processors to enter into a DPA imposing the same data protection obligations as set out in the DPA onto the sub processor in written or electronic form (Art. 28 (4) GDPR).

The DPA obligates the processor to use only (sub)processors providing sufficient guarantees acc. to Art. 28 (1) GDPR (Art. 28 (4)(1) GDPR).

The DPA holds the processor fully liable for when the (sub)processor fails to fulfil its data protection obligations (Art. 28 (4)(2) GDPR).

3.7.1.2.13 Data transfer to third countries (Art. 28 (3)(2)(a) GDPR)

The DPA obligates the processor to transfer data to a third country or an international organisation only, if instructed to do so by the scheme applicant (e.g. in the DPA itself), unless required to do so by Union or Member State law to which the processor is subject.

The DPA obligates the processor with regard to all data transfers to a third country to document whether these comply with the specific requirements of Art. 44–49 GDPR, as well as all other requirements of the GDPR.

3.7.2 Use of subprocessors

The scheme applicant has implemented processes to allow the processor the use of (sub)processors only

[18] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 155.
[19] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 156.

after the scheme applicant has issued in form of a written (or electronic) specific or general authorisation:

3.7.2.1 Specific authorisation

In case of a specific authorisation the scheme applicant specifies which subprocessor and what processing activity it refers to specifically. Any subsequent change, concerning either the type of processing or the person of the sub processor in this case will need to be further authorised by the controller before it is put in place.[20]

3.7.2.2 General authorisation

In case of a general authorisation the controller generally allows the use of sub processors for certain processing operations by providing a list with such sub-processors in an annex thereto.[21]

3.8 Criteria concerning the use of joint controllers

Requirement in a nutshell:
The SA enters into a joint controller agreement with all parties with which it jointly determines the purposes and essential means of processing.

Relevant legal norms:
Art. 26, Art. 4 (7), Art. 5 (2), Art. 12 (1), Art. 13 (1)(a), Art. 30 (1)(a) GDPR **Application criteria**

The SA enters into a joint controller agreement with all parties with which it jointly determines the purpose and sub-purposes and essential means of processing.

3.8.1 Valid Joint Controller Agreement (JCA)

The scheme applicant enters with all joint controllers into a valid JCA, conforming to the following requirements:

3.8.1.1 Valid written or electronic agreement

The JCA is issued in written or electronic form.[22] All essential requirements for the validity of the contract are met. In particular, the written or electronic signature by a natural person who is authorised to represent the company is given.

3.8.1.2 The JCA conclusively attributes responsibility (Art. 26 (1) GDPR)

The joint controller agreement clearly determines for each contracting party (the scheme applicant and the other joint controller) responsibilities for complying with the obligations under the GDPR, in particular:[23]

- the implementation of general data protection principles (Art. 5 GDPR)
- the legal basis of the processing (Art. 6 GDPR)
- the transparency requirements referred to in Art. 13 and 14 GDPR
- the data subject rights, while clarifying that all joint controllers must act on the request of a data

[20] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 155.
[21] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 156.
[22] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 173; although not explicitly imposed by law, due to transparency and notification requirements written or electronic form are factually mandatory - see also: Spoerr in: Wolff/Brink, Art. 26 Rn. 29; Hartung in: Kühling/Buchner, Art. 26, Rn. 26.
[23] See the recommendation of the EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 166.

subject, irrespective of the internal distribution of responsibility (Art. 26 (3) GDPR)
- the security measures (Art. 32 GDPR)
- the notification of a personal data breach to the supervisory authority and to the data subject (Art. 33 and 34 GDPR)
- the data protection impact assessments (Art. 35 and 36 GDPR)
- the use of a processor (Art. 28 GDPR)
- the transfer of data to third countries
- the responsible entity and contact persons for the communication with data subjects, supervisory authorities and the CAB.

The JCA clearly allocates responsibility for different processing operations or parts of processing operations between all involved joint controllers. This includes information on
- the specific duties of each joint controller in order to fulfil the processing purposes,
- the specific means used for processing operations which are being performed by each controller to fulfil these duties,
- the limits regarding the processing of personal data, especially regarding
    - the storage period and time of erasure
    - purpose limitation (prohibiting all joint controllers to process the personal data for other purposes than those covered by this scheme).

3.8.2 Processes to assess the attribution of responsibility between joint controllers

The scheme applicant has implemented a process to assess whether the attribution of responsibility as determined in the JCA actually reflects the respective roles and relationships of the joint controllers vis-à-vis the data subjects (Art. 26 (2) GDPR).

Proof / Evidence	Assessment methods
• Joint controller agreement	• Formal document check and legal review (to clarify unclear terms)

4. Purpose specification and limitation with respect to its processing operation

Requirement in a nutshell:
The SA correctly specifies the purpose and sub-purposes of the data processing operations and limits the processing operations to these purposes.

Relevant legal norms:
Art. 4 (1), (9), Art. 5 (1)(b),(c),(e), Art. 5 (2), Art. 6 (1)(a), Art. 25 (1), Art. 12 (1), 13 (1)(c), Art. 30 (1)(b), Art. 32 GDPR

Specific criteria

The scheme applicant has implemented processes to ensure that all purposes for which it processes personal data are (in view of the specific processing operation):[24]

- **explicit**, requiring the purpose to be sufficiently unambiguous and clearly expressed;
- **legitimate**, requiring the purpose to be compatible also with other areas of law as well as with the data subjects' reasonable expectations and
- **specified**, requiring the purpose to be sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation.

4.1 Proper purpose specification and limitation with respect to its processing operation

Within the scope of application of this Scheme, the purpose of the processing shall be limited by the SA to:

> **Health and treatment data originating from a clinical institution are to be data-minimised or fully anonymised to allow for disclosure by transmission, dissemination or otherwise making available to third parties for downstream purposes.**

As the ToE includes only processing operations conducted by the SA for sub-purposes which can be subsumed under this purpose, the respective sub-purposes have to be specified here in such a way that the SA can show that these sub-purposes can be subsumed under the main purpose.

4.1.1 Proper purpose specification

The SA has implemented processes to properly specify the processing purpose and sub-purposes with reference to the given scope (as defined in chapter I) and to the risks associated with the data processing.

Proof / Evidence	Assessment methods
• Record of processing activities • List of specified processing purpose and sub-purposes	• Formal document check • Legal review (to clarify unclear terms)

4.1.2 Proper purpose limitation assurance

The scheme applicant has implemented processes to identify relevant purpose changes and assess whether the defined processing operations are compatible with the specified purposes (see II.4.1.1).

These processes take into account:

- Any link between the purposes for which the personal data have been collected and the purposes

[24] See Art. 29 Data Protection Working Party, Opinion on purpose limitation, WP203, p. 12.

of the intended further processing;
- The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- The nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Art. 9 GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Art. 10 GDPR;
- The possible consequences of the intended further processing for data subjects;
- The existence of appropriate safeguards, which may include encryption or pseudonymisation.

These processes contain a mechanism to monitor each change of the technical and organisational system used to pursue the purpose in order to discover risks that add to those assessed in the original purpose specification process (see II.4.1.1).

This mechanism must at least take into account changes to one or more of the following aspects:
- The wording of a specific purpose
- The data receivers
- The categories of data categories processed for a purpose
- Other parts of the technical process

The concept must apply the following risk assessment methodology:
- If the changes do not cause a higher or another risk then originally assessed, the change is compatible with the original purpose and can therefore be based on the original legal basis.
- If the changes lead to a higher risk or another risk but can be mitigated (i.e. reduced to the original risk) through technical and/or organisational measures, the changes are compatible with the original purpose and can therefore be based on the original legal basis. The data subjects shall in these cases be informed, if possible.
- If the changes lead to a higher risk that cannot be mitigated (i.e. reduced to the original risk) the SA must demonstrate a new legal basis (e.g. retrieve consent again).

Proof / Evidence	Assessment methods
• Record of processing activities • Access and authorisation concept • Data minimisation or anonymisation concept • Data disclosure concept • List of specified processing purpose and sub-purposes	• Formal document check • Legal review (to clarify unclear terms)

4.2 Data protection by design

The scheme applicant has implemented measures to ensure that all data is processed in a way that is not incompatible with the original purposes (purpose limitation).

The SA takes account of data protection by design by specifying the purpose for which it processes personal data as narrow as possible, added by more detailed sub-purposes.

Such sub-purposes may relate, for example, to ensuring data quality, or backups.

Proof / Evidence	Assessment methods
• List of specified processing purpose and sub-purposes	• Formal document check • Legal review (to clarify unclear terms)

4.3 Transparency

The SA has implemented measures to make all necessary information on the processing purpose publicly available in a precise, transparent, comprehensible and easily accessible form in clear and understandable language.

Proof / Evidence	Assessment methods
• Information in various languages on the SA's website	• Formal document check • Readability assessment

4.4 Documentation

The SA documents:

- all considerations and decisions made for specifying processing purpose
- all organisational measures implemented to ensure compliance with the specific purpose limitation requirements
- the information provided to data subjects concerning the processing purpose

Proof / Evidence	Assessment methods
• Written justification for the specification of processing purpose and sub-purposes • Documentation of organisational measures (text, tables) • Documentation of provided information (text, tables)	• Formal document check • Legal review

4.5 Monitoring

The SA has implemented monitoring measures to ensure that the processing complies with the specific purpose limitation requirements.

Proof / Evidence	Assessment methods
• Record of compliance measures taken (activities, responsibilities, dates) • Review record documentation • Random sample after 1 year	• Formal document check • Legal review (to clarify unclear terms) • Audit (org): Interview with DPO

5. Mandatory data protection impact assessment

Requirements in a nutshell:
The SA assesses all risks caused to the fundamental rights of the data subject and identifies effective measures to address these risks.

Relevant norms:
Art. 35, Art. 5 (1)(a),(b), Art. 5 (2), Art. 24 (1), Art. 25 (1) GDPR **General criteria**

5.1 Processes to assess risks and benefits

5.1.1 Risk assessment organisation

1. The SA has specified clearly and transparently:
    1. who is responsible for conducting the DPIA;
    2. who is part of the team that conducts the DPIA;
    3. what roles play the DPO and/or the project's own DP coordinator or specialist;
    4. who formally accepts the outcome of the DPIA.
2. The SA has specified clearly and transparently what the process looks like and in which order which steps are taken.
3. The SA has implemented formats and methods to seek the views of data subjects or their representatives on the intended processing.
4. The SA has implemented procedures and methods to:
    1. systematically describe the envisaged processing operations and the purpose and sub-purposes of the processing;
    2. assess the necessity and proportionality of the processing operations in relation to the purpose and sub-purposes;
    3. identify and assess the risks to the rights and freedoms of data subjects;
    4. identify the measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of fundamental rights and to demonstrate compliance with the GDPR;
    5. include compliance with approved codes of conduct in accordance with Article 40 GDPR in risk identification, assessment and mitigation.

5.1.2 Identification of risks to fundamental rights

The SA has implemented procedures and methods to identify and assess all risks to the fundamental rights and freedoms of data subjects posed by the data processing in the full scope of chapter I of this scheme.
The risk assessment covers at least the risks to the fundamental rights and freedoms referred to in section I. 2.1.3 of this scheme.

5.2 Mandatory requirements specific to the DPIA

The SA has implemented processes to perform assessments according to Article 35(2) GDPR with the help of its DPO, taking into account:

1. potential compliance with approved codes of conduct referred to in Article 40 GDPR by the relevant controllers or processors;
2. the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

This mandatory assessment contains at least:

- a systematic listing of those processing operations and (sub-)purposes of the processing described in the record of processing activities according to Article 30 GDPR;
- a clear and transparent description of the methods and measures used for creating the record of processing activities;
- an assessment of the necessity and proportionality of the processing operations in relation to the (sub-)purposes;
- an assessment of the risks to the fundamental rights and freedoms of data subjects referred to in section II. 5.1.2;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR and other applicable data protection laws taking into account the rights and legitimate interests of data subjects and other persons concerned; and
- a graphical representation of the processing activities (e.g. use case diagram), the actors involved, the systems used for processing the data, the data flows, the risks to the rights and freedoms of data subjects connected to or associated with the different processing steps, and the measures envisaged to address (i.e., prevent, mitigate or compensate for) these risks.

5.3 Data protection by design

The SA has implemented risk identification and assessment procedures and methods which correspond to the state of the art.

The SA ensures that the measures envisaged to address the identified risks are effective in preventing, mitigating and/or compensating for these risks, and correspond to the state of the art.

Proof / Evidence	Assessment methods
• Literature review wrt the state of the art of conducting DPIA • Literature review wrt the state of the art of the measures, their efficacy and effectiveness, envisaged to address the risks	• Formal document check • State of the art review • Interviews with DPO and the DPIA team members

5.4 Transparency

The SA has implemented procedures and methods to ensure that the specification as well as the process and outcome documentation of the DPIA are in a transparent, intelligible and easily accessible form.

Proof / Evidence	Assessment methods
• DPIA specification: 1) roles and responsibilities, 2) processes, 3) methods, 4) data subjects' or their representatives' participation • Documentation of the DPIA process (planning & preparation, conduct, results), including participatory formats • DPIA results (texts, tables, diagrams)	• Formal document check • Readability assessment

5.5 Documentation

The SA has implemented measures to document:

- specifications of the DPIA, including
  - roles and responsibilities wrt to the planning, preparation, conduct and documentation of the DPIA,
  - processes of the planning, preparation, conduct and documentation of the DPIA,
  - methods to be applied when conducting the DPA, and
  - the participation of the data subjects;
- the process and the outcome of the DPIA; and
- the results of the DPIA (texts, tables, and diagrams).

Proof / Evidence	Assessment methods
• DPIA specification: 1) roles and responsibilities, 2) processes, 3) methods, 4) data subjects' or their representatives' participation • Documentation of the DPIA process (planning & preparation, conduct, results), including participatory formats • DPIA results (texts, tables, diagrams)	• Formal document check • Legal review

5.6 Monitoring

The SA monitors whether the identification and assessment of the risks as well as the measures envisaged to address these risks remain appropriate over time and against the backdrop of changing contexts, technological progress, and social development.

Proof / Evidence	Assessment methods
• Periodic review specification • Review documentation • Random sample after 1 year	• Formal document check • Audit (org): Interview with DPO

6. Legal basis according to the GDPR

Requirement in a nutshell:
The SA specifies a legal basis for each purpose of processing.
If the legal basis is the consent of the data subjects pursuant to Article 6(1)(a) GDPR, the SA provides a mechanism to allow the withdrawal of consent.

Relevant legal norms:
Art. 4 (11), Art. 6 (1)(a), Art. 7, Art. 12, Art. 13, Art. 22 (2)(c), Art. 44 ff., Art. 25 (1), Art. 5 (2) GDPR, § 6 (3)(3) Gesundheitsdatennutzungsgesetz

Specific criteria

6.1 Legal basis specification

The SA specifies, for each purpose of processing, one of the legal bases listed in Article 6(1) GDPR, unless a more specific statutory legal basis is applicable:

- informed consent of the data subjects, particularly patients;
- performance of a contract or steps taken prior to entering into a contract;
- compliance with a legal obligation to which the controller is subject;
- protection of the vital interests of the data subjects;
- necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- necessity for the purposes of the legitimate interests pursued by the controller or a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects requiring the protection of personal data.

If the legal basis is the consent of the data subjects pursuant to Article 6(1)(a) GDPR, the SA provides an explicit overview of the benefits and risks associated with the processing to the data subjects as well as, if applicable, an easy-to-use mechanism to allow the withdrawal of consent.

If the legal basis is the performance of a contract pursuant to Article 6(1)(b) GDPR, the SA ensures that the contract contains an explicit clause outlining the processing and its purpose, its associated benefits and risks as well as where to find additional information.

If the legal basis is the legitimate interests pursuant to Article 6(1)(f) GDPR, the SA ensures that those interests are limited to the purpose specified in chapter I of this scheme.

If one of the legal bases listed in Article 6(1) GDPR is chosen, the SA demonstrates that no more specific statutory legal basis is applicable.

If the legal basis is pursuant to § 6 (3)(3) Gesundheitsdatennutzungsgesetz, the SA ensures that the anonymisation of personal data by data-processing healthcare institutions and the transmission of anonymised data to third parties is in accordance with medical, rehabilitative and nursing research purposes.

6.2 Data protection by design

The SA has implemented adequate procedures and methods to ensure that the data subjects are not overburdened with decisions for which they lack a sufficient basis for decision-making. This means, in particular, that the controllers shall not shift their responsibility for the risks to fundamental rights and

freedoms, as well as their mitigation, onto the data subjects.

Proof / Evidence	Assessment methods
• Data protection concept • Data protection impact assessment documentation • Record of processing activities • Separate listing of data protection requirements	• Formal document check • Legal review

6.3 Transparency

The SA has implemented adequate measures to ensure that the information to the data subjects concerning the processing and its legal basis, including the information required in connection with specific legal bases, is in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and enables data subjects to easily derive and/or understand the risks associated with the processing.

Proof / Evidence	Assessment methods
If applicable, • informed consent form within the treatment contract, or • information on data processing within the treatment contract In addition: • Information in the general terms and conditions • Separate information on data storage period and data transfer • Specification of the legal basis in the data protection policy • Explicit and publicly available presentation of the balancing of interests • Risk derivation and understanding assessment, if possible, including user testing results	• Formal document check • Legal review • Readability assessment

6.4 Documentation

The SA has implemented measures to document:

- the rationale behind the particular selection of the legal basis in contrast to other options available,
- the information provided to data subjects concerning the legal basis of the processing, including, if applicable, the informed consent form,
- the specification, planning, conduct and results of the risk derivation and understanding assessment, including, if applicable, user testing results, and,
- if the legal basis is the consent of the data subjects pursuant to Article 6(1)(a) GDPR, the withdrawal of consent by data subjects.

Proof / Evidence	Assessment methods
• Record of processing activities • Justification of the selection of the specific legal basis • Risk derivation and understanding assessment, if possible, including user testing results • Withdrawal of consent documentation (if applicable)	• Formal document check • Legal review

6.5 Monitoring

The SA has implemented measures to ensure that the processing complies with the specific requirements stipulated by the particular legal basis.

The SA has implemented measures to ensure the periodic review and, if necessary, revision of the information provided to data subjects.

The SA has implemented measures to ensure the periodic review of development concerning data-related legislation.

Proof / Evidence	Assessment methods
• Periodic review specification • Review documentation • Random sample after 1 year	• Formal document check • Legal review

7. Data minimisation / anonymisation

Requirement in a nutshell:
The SA preprocesses personal data in order to minimise or anonymise the data to some expected degree for subsequent disclosure.

Relevant legal norms:
Art. 2 (1), Art. 4 (1), Art. 5 (1)(c), (e), Art. 24 (1), Art. 25 (1), Art. 5 (2) GDPR **General criteria**

7.1 Processes to assess the data minimisation principle

The SA has implemented measures to assess:

1. whether it only processes personal data that is adequate, relevant and limited to what is necessary for achieving the intended purpose and sub-purposes (see 4. Purpose specification and limitation with respect to its processing operation),[25] and
2. how to achieve the intended objectives according to the chosen option, (a) data minimisation or (b) anonymisation (see chapter I. 2.1 Purpose and processing operations).

This assessment includes:

- an evaluation to what degree the data subject needs to be identifiable in order to achieve the intended purpose. In this assessment, the SA assesses whether it can achieve this purpose also by only processing pseudonymised data and if so, determines the earliest point in time when pseudonymisation of personal data is feasible.[26] (see also II.14. Data protection by design)
- an evaluation to what degree the personal data is to be minimised or anonymised before disclosure by transmission, dissemination or otherwise making available to third parties, and what measures, procedures, metrics, and tools are available to achieve that degree of data minimality or anonymity.

7.2 Data protection by design

The SA has specified and implemented effective measures to make personal data and/or identifiers accessible only to a minimal number of people which are sufficiently trained and informed about securely handling the data (access and authorisation concept).

[25] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 73.
[26] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 75.

The SA has implemented measures to assess the type and characteristics of the personal data to be minimised or anonymised.

The SA has implemented measures to assess downstream processing contexts and purposes as well as the intended applications, which particularly allow for defining suitability and thus expected quality of the data to be shared.

The SA has implemented measures to assess the characteristics and statistical properties of the data that is required for the envisaged purposes and intended applications.

The SA has specified a suitable attacker model & threat model and provided justification for selecting them with regards to downstream contexts, recipients, purposes and processing operations.

Option (a) data minimisation	**Option (b) anonymisation**
Attacker & threat model: the SA has to define the set of legitimate recipients, taking into account that neither further dissemination nor third-country transfer are allowed, and the downstream purposes are limited to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).	Attacker & threat model: the SA has to presume that the attacker has • full access to anonymised data, • no access to any intermediate step or output in the preprocessing stage, and • partial information on some (original) data subjects.

The SA has implemented procedures and methods to identify and assess all risks to the data, the minimality or anonymity of the data, and the compliance with applicable data protection regulation originating in the downstream contexts.

The SA has selected effective data minimisation and/or anonymisation measures, procedures, metrics, and tools that are adequate for the intended degree of data minimality or anonymity against the backdrop of the results of the aforementioned risk analysis.

Option (a) data minimisation	**Option (b) anonymisation**
The SA has to select appropriate and reasonably up-to-date ta minimisation, pseudonymisation & anonymisation guidelines that address practitioners wrt the selection of adequate data minimisation methods, metrics, and tools, and	The SA has to conduct a full-fledged literature review wrt the state of the art of • anonymising data and anonymisation methods,

follow the guidance. Examples of appropriate guidelines include: • Article 29 Data Protection Working Party (2014), *Opinion 05/2014 on Anonymisation Techniques*, WP216. • European Union Agency for Cybersecurity (ENISA) (2021), *Data Pseudonymisation. Advanced Techniques and Use Cases.* • Schwartmann et al. (2022), *Praxisleitfaden für die Anonymisierung personenbezogener Daten – Anforderungen, Einsatzklassen und Vorgehensmodell*. Leipzig: Stiftung Datenschutz. • European Data Protection Board (EDPB) (2025), *Guidelines 01/2025 on pseudonymisation.*	• anonymity metrics and testing, • the expected degree of anonymity for the specific context and wrt the specific data, and • tools or toolchains for supporting anonymisation and testing.

The SA has specified and implemented effective measures to delete all direct or indirect identifiers and/or raw data as soon as identification is no longer needed and/or these identifiers are not necessary for the intended purposes and applications.[27]

The SA has specified and implemented effective measures:
- to apply data minimisation and/or anonymisation procedures,
- to test and assess outcomes, both regarding the quality and the degree of data minimality or anonymity of the data,
- and to repeat if necessary until the achieved degree of data minimality or anonymity meets the expected / specified degree.

Option (a) data minimisation	**Option (b) anonymisation**
Conduct one or more steps of • generalisation • randomisation procedures. If applicable, use the output data to train one or more generator models, and use the model(s) to create synthetic data.	Conduct one or more steps of • generalisation • randomisation procedures. Use the output data to train one or more generator models, and use the model(s) to create synthetic data.

[27] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 75.

Beware that randomisation methods might weaken or destroy (statistically significant) relationships between individual data, items, and/or values. Use with care. Test and assess the quality of the data and the degree of data minimality. In particular, assess the quality of the data and the data minimality not only for the average but also regarding the worst case as well as their fairness, i.e. apply fairness metrics and, if applicable, XAI methods to subgroups and clusters. Repeat this process until the achieved degree of data minimality meets the expected / specified degree.	Beware that randomisation methods might weaken or destroy (statistically significant) relationships between individual data, items, and/or values. Use with care. Test and assess the quality and the degree of anonymity of the data. In particular, assess the quality and the anonymity of the data not only for the average but also regarding the worst case as well as their fairness, i.e. apply fairness metrics and XAI methods to subgroups and clusters. Repeat this process until the achieved degree of anonymity meets the expected / specified degree.

Proof / Evidence	**Assessment methods**

• Data flow diagram
• Access and authorisation concept
• Data minimisation / anonymisation concept, incl.
  ○ input data type, characteristics and quality assessment concept,
  ○ data minimisation / pseudonymisation / anonymisation methods, metrics and procedure concept
  ○ synthetic data generation concept
  ○ output data quality and minimality / anonymity assessment concept
• On request: access to IT system
	• Formal document check
	• Legal and technical review
	• Audit (org): interview with DPO

7.3 Documentation

The SA has implemented measures to document these assessments and implemented measures (see 2. Documentation).

Proof / Evidence	**Assessment methods**

• Access and authorisation protocol • Deletion protocol • Minimisation / pseudonymisation / anonymisation protocol • Synthetic data generation protocol • Synthetic data quality and minimality / anonymity assessment protocol	• Formal document check • Legal and technical review • Audit (org): Interview with DPO

7.4 Monitoring

The SA has implemented measures to detect changes of the state of the art in data minimisation, anonymisation and synthetisation.

Proof / Evidence	Assessment methods
• Literature review • Eventually updated documentation • Random sample after 1 year	• Formal document check • Legal and technical review • Audit (org): Interview with DPO

8. Rule setting, binding and enforcement

Requirement in a nutshell:
The SA selects a platform for making data available that guarantees the setting of adequate rules and their enforcement against the data recipients, given their consent to the set of rules.

Relevant legal norms:
Art 28 (1), (3), 32 GDPR

Specific criteria

8.1 Rule setting, binding and enforcement

The SA has selected a platform that has set an adequate set of rules for users of the platform on the basis of applicable law and, given their consent, demonstrably enforces these rules to detect, evaluate, and sanction violating user behaviour.

8.1.1 Rule setting

The SA has selected a platform that has set an adequate set of rules for users of the platform on the basis of applicable law.

Proof / Evidence	Assessment methods
• Set of rules for users of the platform • List of legal bases	• Formal document check • Legal review

8.1.2 Rule binding

The SA has selected a platform that has implemented measures to ensure that platform users and data recipients are obliged to read the set of rules, meet these obligations, and are bound to them.

Proof / Evidence	Assessment methods
• Documentation of the rules provided or made accessible to data recipients • Consent documentation	• Formal document check • Legal review

8.1.3 Rule enforcement

The SA has selected a platform that demonstrably enforces the set of rules to detect, evaluate, and sanction violating user behaviour depending on severity, frequency (e.g. repetition) and culpability (intent and negligence) of violations.

Proof / Evidence	Assessment methods
• Rule violation detection concept • Rule violation evaluation concept • Rule violation sanctioning concept • Record of sanctions	• Formal document check • Legal review

8.2 Data protection by design

The SA has selected a platform that takes account of data protection by design by preventing rule violations by users as best as possible via technical measures.

Proof / Evidence	Assessment methods
• Technical concept for the prevention of rule violations by users • Separate listing of technical data protection measures	• Formal document check • Legal review (to clarify unclear terms)

8.3 Transparency

The SA has selected a platform that has implemented measures to make all necessary information on the introduced set of rules and its enforcement against data recipients publicly available in a precise, transparent, comprehensible and easily accessible form in clear and understandable language.

Proof / Evidence	Assessment methods
• Information in various languages on the SA's website	• Formal document check • Readability assessment

8.4 Documentation

The platform documents:

- all measures taken to detect violating user behaviour
- all measures taken to evaluate violating user behaviour
- all measures taken to sanction violating users
- the information provided to violating users concerning the SA's rule enforcement

Proof / Evidence	Assessment methods
• Detection protocol • Evaluation protocol • Sanctioning protocol • Documentation of information provided to violating users (text, tables)	• Formal document check • Legal review

8.5 Monitoring

The SA has implemented measures to ensure that the setting and enforcement of rules by the platform complies with the applicable law.

Proof / Evidence	Assessment methods
• Record of compliance measures taken (activities, responsibilities, dates) • Questionnaires • Review record documentation • Random sample after 1 year	• Formal document check • Legal review (to clarify unclear terms) • Audit (org): Interview with DPO

9. Identifiability of the data recipient

Requirement in a nutshell:
The SA selects a platform for making data available that ensures that all data recipients are identifiable and their identity is proven before data is made available to them.

Relevant legal norms:
Art 28 (1), (3), 32 GDPR **Specific criteria**

9.1 Identification and authentication

The SA has selected a platform for making data available that ensures that all data recipients are identifiable and their identity is proven before data is made available to them.

9.2 Data protection by design

The SA has selected a platform that has implemented adequate procedures and methods to ensure that all data recipients are identifiable by their name, contact details, and, if applicable, purpose of data use. In particular, the platform must ensure that the data recipients' identities are proven before they get access to data.

Proof / Evidence	Assessment methods
• List of data recipients' names • List of data recipients' contact details • List of data recipients' purposes of data use • Identification checklists	• Formal document check • Legal review

9.3 Transparency

The SA has selected a platform that has implemented measures to make all necessary information on the procedures and methods taken to ensure identifiability of the data recipient publicly available in a precise, transparent, comprehensible and easily accessible form in clear and understandable language.

Proof / Evidence	Assessment methods
• Information in various languages on the SA's website	• Formal document check • Legal review • Readability assessment

9.4 Documentation

The SA has implemented measures to document:
- measures to identify data recipients.

Proof / Evidence	Assessment methods
• proofs of identity of the data recipients • documentation of the identification process	• Formal document check • Legal review

9.5 Monitoring

The SA monitors whether the platform is in the position to make all data recipients identifiable by their name, contact details, and purpose of data use at any time.

Proof / Evidence	Assessment methods
• Periodic review specification • Review documentation • Random sample after 1 year	• Formal document check • Legal review

10. Purpose specification and limitation with respect to the data re-use

Requirement in a nutshell:
The SA has selected a platform for making data available that ensures the correct specification, transparency, and limitation of the purpose and sub-purposes of the data re-use.

Relevant legal norms:
Art. 5 (1)(c),(e), 6 (1), 25 (1), 14 GDPR **Specific criteria**

10.1 Purpose specification, transparency and limitation

The SA has selected a platform that has specified the purpose and sub-purposes for which it allows or forbids the re-use of data that is disclosed to data recipients, and has implemented measures to ensure that the purposes and sub-purposes are made transparent.

10.1.1 Transparency of the re-use purposes

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to require data recipients to disclose all necessary information about the processing purposes and sub-purposes to the platform and the public in a precise, transparent, comprehensible and easily accessible form in clear and understandable language, e.g. on their websites.	

10.1.2 Purpose limitation for re-use

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to ensure that data recipients only re-use data that is made available to them for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law.	

10.1.3 Impermissible purposes

The SA has selected a platform that has implemented measures to ensure that data recipients do not re-use data to derive insights about the economic situation, assets and activities of the health or care institutions that provide the data or, where applicable, the data holder.

10.2 Data protection by design

The SA has selected a platform that takes account of data protection by design by specifying the purpose for which it allows re-use of personal data as narrow as possible, added by more detailed sub-purposes.

Such sub-purposes may relate, for example, to ensuring data quality, or backups.

Proof / Evidence	Assessment methods
• List of specified processing purposes and sub-purposes	• Formal document check • Legal review (to clarify unclear terms)

10.3 Documentation

The SA has selected a platform that documents:

- all considerations and decisions made for specifying the processing purpose and sub-purposes
- all organisational measures implemented to ensure compliance with the specific purpose limitation requirements
- the information provided to data subjects concerning the processing purpose and sub-purposes

Proof / Evidence	Assessment methods
• Written justification for the specification of the processing purpose and sub-purposes • Documentation of organisational measures (text, tables) • Documentation of provided information (text, tables)	• Formal document check • Legal review

10.4 Monitoring

The SA has selected a platform that has implemented monitoring measures to ensure that the data re-use complies with the specific purpose limitation requirements.

Proof / Evidence	Assessment methods
• Record of compliance measures taken (activities, responsibilities, dates) • Review record documentation • Random sample after 1 year	• Formal document check • Legal review (to clarify unclear terms) • Audit (org): Interview with DPO

11. Information to data recipients

Requirement in a nutshell:
The SA selects a platform for making data available that provides data recipients with all necessary information for data re-use.

Relevant legal norms:
Art. 19, Art. 24 (1), 25 (1), 28, 32 (1), Art. 44 – 49 GDPR **Specific criteria**

11.1 Information to data recipients

The SA has selected a platform that provides data recipients with information about statistical data properties (or purpose and population properties), marginal cases, edge cases, or fairness problems.

The SA ensures that the platforms have all this information at their disposal.

11.2 Data protection by design

The SA has selected a platform that implemented measures to provide each data recipient with all necessary information in a clear and understandable way.

Proof / Evidence	Assessment methods
• Detailed information sheet for data recipients in various languages with all necessary information for data re-use • Public website in various languages with all necessary information for data re-use	• Formal document check • Legal review • Readability assessment • Audit (org)

11.3 Documentation

The SA has selected a platform that documents fulfilment of all transparency requirements at hand.

Proof / Evidence	Assessment methods
• Documentation of provided information via sheets (text, tables) and time of information	• Formal document check • Legal review

11.4 Monitoring

The SA has selected a platform that monitors compliance with the transparency requirements at hand.

Proof / Evidence	Assessment methods
• Periodic review • Review documentation • Random sample after 1 year	• Formal document check • Legal review

12. No linking

Requirement in a nutshell:
The SA does not link anonymous data to personal data.

Relevant legal norms:
Art. 1, Art. 2 (1), 24 (1), 25 (1) GDPR

General criteria

12.1 No linking

Option (a) data minimisation	Option (b) anonymisation
	The SA selects a platform that ensures that the data recipients do not link anonymous data to personal data downstream.

12.2 Documentation

The SA has selected a platform that documents the measures taken to ensure that the data recipients do not link anonymous data to personal data downstream.

Proof / Evidence	Assessment methods
• Documentation of the rules provided or made accessible to data recipients • Consent documentation	• Formal document check • Legal review

12.3 Monitoring

The SA has selected a platform that monitors compliance with ensuring that the data recipients do not link anonymous data to personal data downstream.

Proof / Evidence	Assessment methods
• Periodic review • Review documentation • Random sample after 1 year	• Formal document check • Legal review

13. Population and purpose compatibility

Requirement in a nutshell:
The SA selects a platform that observes the compatibility of populations and purposes.

Relevant legal norms:
Art. 6 (4), 13 (1)(f), 30 (1)(e), 4 (1), Art. 44 – 49 GDPR

Specific criteria

13.1 Population and purpose compatibility

The SA has selected a platform that observes the compatibility of populations and purposes.

Option (a) data minimisation	Option (b) anonymisation
	The SA selects a platform that has implemented measures to ensure that data recipients do not use models trained on data directly in practice without adequate assessment of the suitability. The SA selects a platform that has implemented measures to ensure that data recipients pay special attention to the possible violation of the basic assumption of equal statistical distribution of the populations, but also the purpose-related quality assurance limits.

13.2 Documentation

The SA has selected a platform that documents the measures taken to ensure that the data recipients do not use models trained on data directly in practice without adequate assessment of the suitability, and pay special attention to the possible violation of the basic assumption of equal statistical distribution of the populations, but also the purpose-related quality assurance limits.

Proof / Evidence	Assessment methods
• Documentation of the rules provided or made accessible to data recipients • Consent documentation	• Formal document check • Legal review

13.3 Monitoring

The SA has selected a platform that monitors compliance with ensuring that the data recipients do not use models trained on data directly in practice without adequate assessment of the suitability, and pay special attention to the possible violation of the basic assumption of equal statistical distribution of the populations, but also the purpose-related quality assurance limits.

Proof / Evidence	Assessment methods
• Periodic review	• Formal document check

• Review documentation • Random sample after 1 year	• Legal review

14. Data protection by design

Requirement in a nutshell:
The SA selects a platform that has implemented appropriate technical and organisational measures.

Relevant norms:
Art. 25 (1) GDPR — **General Criteria**

Processes to specify the technical and organisational measures

The SA has selected a platform that has implemented measures to assess risks of re-identification, linkability, inference attacks and singling-out concerning the metrics used which should cover the worst case, and the fairness of data minimisation and anonymisation.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that conducts and submits a list of fundamental rights affected and a fundamental rights-specific voluntary commitment to risk-management.	

The SA has selected a platform that regularly repeats the risk assessment, in particular with regards to the technical and scientific developments in the field of anonymisation and re-identification as well as fairness.

The SA has selected a platform that adequately specifies what it considers "regularly", and justifies it.

The SA has selected a platform that has implemented measures to stop data sharing in the case of a negative outcome of the risk assessment.

The SA has selected a platform that has implemented processes to specify the appropriate technical and organisational measures to implement data-protection principles effectively and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. This specification takes into account:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of the processing;
- the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (see 5. Data protection impact assessment).

Remark:
The implementation of effective measures to implement the data protection principles are in this scheme assessed already for each criteria individually. The function of this criteria thus serves as an overall assessment, whether the entirety of technical and organisational protection measures effectively decrease the risks to fundamental rights of data subjects.

Due to the vague and normative character of this cross-criteria assessment, empirical methods in this case are not suited as proof to determine the "overall" effectiveness of the technical and organisational

system. The assessment is thus limited to identifying **protection gaps**, which might remain despite effective data protection by design regarding each individual criteria.

The benchmark for this review of protection gaps is that, as a result of the processing of personal data, no further risks may be caused to the fundamental rights of the data subject compared to those specified in the scope[28]. All remaining risks must also be effectively controlled with technical and organisational measures.

The SA has selected a platform that specifies these measures already at the time of determining the means for processing and latest at the time of the processing itself (Art. 25 (1) GDPR).

The SA has implemented measures to ensure that all processing operations that are not covered by the DPIA (see chapter 5), are:

- listed and documented;
- assessed regarding the risks they pose;
- have their risks covered by measures taken or envisaged.

Proof / Evidence	Assessment methods
• If applicable, the list of all processing operations that are not covered by the DPIA • If applicable, risk assessments with associated protection measures	• Formal document check • Interview with DPO

[28] see I. Scope.

15. Re-Identification prohibition

Requirement in a nutshell:
The SA ensures that data recipients & re-users will prevent the re-identification of data.

Relevant legal norms:
Art. 13 (1)(f), 30 (1)(e), 4 (1), Art. 44 – 49 GDPR **Specific criteria**

15.1 Re-Identification prohibition

The SA has selected a platform that ensures that data recipients and re-users will prevent the re-identification of data.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that ensures that data recipients and re-users are prohibited from re-identifying any data subject to whom the data relates. The SA has selected a platform that has taken technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body.	

15.2 Documentation

The SA has selected a platform that documents the measures taken to ensure that the recipients and re-users are prevented from the re-identification of data.

Proof / Evidence	Assessment methods
• Documentation of the rules provided or made accessible to data recipients • Consent documentation	• Formal document check • Legal review

15.3 Monitoring

The SA has selected a platform that monitors the compliance with ensuring that the data recipients and re-users are prevented from re-identification of data.

Proof / Evidence	Assessment methods
• Documentation of the rules provided or made accessible to data recipients • Consent documentation	• Formal document check • Legal review

16. Transparency

Requirement in a nutshell:
The SA has selected a platform that provides for the fulfilment of all transparency requirements.

Relevant legal norms:
Art. 12, Art. 5 (1)(a), Art. 5 (2), Art 22 (1), Art. 24 (1) GDPR **Specific criteria**

16.1 Information according to Art. 14 GDPR

The SA has selected a platform that has implemented measures to fulfil all transparency requirements, including providing public information, e.g. on the platform's and the data recipient's websites.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that provides for the fulfillment of all transparency requirements according to Art. 14 GDPR, including: • the identity and the contact details of the platform and the data recipients; • the purposes of the processing for which the personal data are intended; • the legal basis for the processing; • the categories of personal data concerned; • the period for which the personal data will be stored; • the legitimate interests pursued by the controller; • the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject; • the existence of the right to object to processing as well as the right to data portability; • the existence of the right to withdraw consent at any time; • the existence of the right to lodge a complaint with a supervisory authority; • from which source the personal data originate; • the non-existence of automated decision-making; • all risks (and potentially benefits) to the exercise of fundamental rights of the data subjects which result from the processing of personal data for the respective	The SA has selected a platform that provides adequate transparency regarding the disclosure of fully anonymised data, the non-applicability of the data protection regulation as well as the fact that nevertheless adequate measures have been taken to ensure that fundamental rights and freedoms are protected, re-identification is excluded pursuant to the state of the art, and data can be retracted if the need arises, e.g., changes in the state of the art of re-identification or a data recipient found to be violating the platform's rules and conditions.

purposes (see II.5. DPIA).	

16.2 Data protection by design (transparent information)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to provide each data subject, in particular patients, with all necessary information (as listed above).	

Proof / Evidence	Assessment methods
• Data protection policy • Public website in various languages with all information listed in chapter 16.1	• Formal document check • Legal review • Readability assessment • Audit (org)

16.3 Documentation

The SA has selected a platform that documents fulfilment of all transparency requirements at hand.

Proof / Evidence	Assessment methods
• Assessment of the burden of providing the information to the data subject versus the impact on and consequences for the data subject if the data subject remains deprived of the information • Documentation of provided legal information	• Formal document check • Legal review • Audit (org): interview with employees

16.4 Monitoring

The SA has selected a platform that monitors compliance with the transparency requirements at hand.

Proof / Evidence	Assessment methods
• Periodic review • Review documentation • Random sample after 1 year	• Formal document check • Legal review

17. Data subject rights

Requirement in a nutshell:
The SA has selected a platform that provides for the fulfilment of the data subject's rights.

Relevant norms:
Art. 12 , Art. 15, Art. 16, Art. 17, Art. 18, Art. 19 (1), Art. 20, Art. 21 , Art. 11, Art. 24 (1), Art. 25 (1), Art. 89 (2)(3), Art. 5, Art. 7 (3) GDPR **General criteria**

17.1 Facilitation of data subject rights

The SA has selected a platform that has implemented measures to provide for and facilitate the exercise of data subject rights, e.g. on the platform's and, if applicable, the data recipient's websites.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to ensure that it is as convenient as possible for the data subjects to exercise their rights, both analogue and digital. The SA has selected a platform that has implemented measures to ensure that the data recipients make it as convenient as possible for the data subjects to exercise their rights, both analogue and digital.	The SA has selected a platform that provides adequate information that the exercise of data subjects rights both proves impossible and is not mandated by the GDPR, as only fully anonymised data is disclosed to third parties.

Measures may include:

- paper-based or electronic forms and templates to be filled by data subjects to exercise one or several data subject's rights;
- one-click solutions (e.g., on the platform's or data recipient's websites) or barcodes (e.g., on paper handouts) for direct access to options to exercise rights; or
- points of contact on site.

Proof / Evidence	Assessment methods
• Literature review wrt the state of the art on enabling and facilitating the exercise of data subjects' rights • Eventually updated documentation • User tests • Random sample after 1 year	• Formal document check • Legal review • Audit (org): Interview with DPO

17.2 Right of access (Art. 15 GDPR)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to provide data subjects	

with confirmation as to whether or not personal data concerning them are being processed upon their request. The SA has selected a platform that has implemented measures to ensure that the data recipients provide data subjects with confirmation as to whether or not personal data concerning them are being processed upon their request. When requested to, the platform and/or the data recipient provides information about the data subject's personal data and the following information listed in Art. 15 para. 1 lit. a) – h) GDPR: • the purposes of the processing; • the categories of personal data concerned; • the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; • where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; • the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; • the right to lodge a complaint with a supervisory authority; • where the personal data are not collected from the data subject, any available information as to their source.	

17.3 Right to rectification (Art. 16 GDPR)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to rectify inaccurate personal data concerning data subjects without undue delay upon request of the data subject. The SA has selected a platform that has	

implemented measures to ensure that the data recipients rectify inaccurate personal data concerning data subjects without undue delay upon request of the data subject. The SA has selected a platform that has implemented measures to complete incomplete personal data concerning the data subject upon request of the data subject, taking into account the purposes of the processing, including by means of providing a supplementary statement. The SA has selected a platform that has implemented measures to ensure that the data recipients complete incomplete personal data concerning the data subject upon request of the data subject, taking into account the purposes of the processing, including by means of providing a supplementary statement.	

17.4 Right to erasure ("right to be forgotten") (Art. 17 GDPR)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to erase personal data concerning the data subject without undue delay upon request of the data subject. The SA has selected a platform that has implemented measures to ensure that data recipients erase personal data concerning the data subject without undue delay upon request of the data subject. In particular, the SA has selected a platform that erases, and ensures that the data recipients erase, personal data if the data subject withdraws their consent or if one of the reasons listed in Art. 17 para. 1 lit. a) – f) GDPR applies: • the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; • the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;	

• the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); • the personal data have been unlawfully processed; • the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; • the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	

17.5 Right to restriction of processing (Art. 18 GDPR)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to restrict, and ensures that the data recipients restrict, the processing if one of the conditions listed in Art. 18 para. 1 lit. a) - d) applies: • the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; • the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; • the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; • the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	

17.6 Right to object (Art. 21 GDPR)

Option (a) data minimisation	Option (b) anonymisation
If the processing of personal data is based on Art.	

6 para. 1 lit. e) or f) GDPR, the SA has selected a platform that has implemented measures to stop, and ensures that the data recipients stop, the processing after the data subject has lodged an objection based on grounds relating to his or her particular situation. This does not apply if the SA, the platform and/or the data recipient can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or if the processing serves the establishment, exercise or defense of legal claims. However, if the processing of personal data is carried out on the basis of Art. 6 para. 1 lit. a) to d) GDPR, the data subject has no right to object pursuant to Art. 21 GDPR.	

17.7 Right to withdraw consent (Art. 7 (3) GDPR)

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that has implemented measures to ensure, and ensures that the data recipients ensure, the data subject's right to withdraw their consent at any time. The SA, the platform and/or the data recipient ensures that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the SA, the platform and/or the data recipient informs the data subject thereof. The SA, the platform and/or the data recipient ensures that it is as easy to withdraw as to give consent.	

18. Storage limitation

Requirement in a nutshell:
The SA has selected a platform that stores personal data only for as long as it is necessary to fulfil the purpose for which it was collected.

Relevant norms:
Art. 5 (1)(e), Art. 13 (2)(a), Art. 24 (1), Art. 35, Art. 25 (1), Art. 30 (1)(f), Art. 89 (1)(1), Art. 5 (2), Art. 4 (1) GDPR[29] **General criteria**

18.1 Retention period

The SA has selected a platform that has implemented measures to limit the storage of personal data for no longer than is necessary for the purposes for which the personal data are processed.

The SA has selected a platform that has specified clearly and transparently the retention period or the deletion conditions.

18.2 Erasure of personal data

The SA has selected a platform that has implemented measures to ensure that the data is deleted as specified and the deletion is documented.

The SA has specified clearly and transparently:
- when the data will be deleted;
- what deletion mechanism or methods will be used;
- who is responsible for deleting the data or configuring an automated deletion mechanism; and
- how the deletion will be documented.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that ensures erasure of personal data if risk assessment requirements are not met.	
The SA has selected a platform that ensures that data recipients erase personal data when the purpose is fulfilled or the data are no longer required (Art. 5(1e) GDPR).	The SA has selected a platform that ensures that data recipients are prepared to erase personal data if the platform, the supervisory authority or a third party proves that the personal data are no longer anonymous and provide sufficient guarantees to actually erase the data.

Proof / Evidence	Assessment methods
• Deletion concept • Deletion protocol • Access and authorisation protocol	• Formal document check • Legal review

[29] Baustein 60 „Löschen und Vernichten“ V1.0a, SDM V2.0, September 2, 2020.

19. Third country transfer

Requirement in a nutshell:
The SA fulfils all third country transfer requirements.

Relevant legal norms:
Art. 44, Art. 45, Art. 46, Art. 47, Art. 49, Art. 13 (1)(f), Art. 30 (1)(e), Art. 4 (1) GDPR

General criteria

No third country transfer

The SA regards data transmissions as third country transfers, if the receiving part and the SA are part of a group of undertakings and the group or the receiving part is located in a third country.[30]

Any country that is not a member of the European Union (EU) or European Economic Area (EEA) is regarded as a third country.[31]

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that does not transmit personal data to third countries or international organisations.	

[30] See Recital 48 (2) GDPR.
[31] See Decision No. 154/2018 of the EEA Joint Committee 6.7.2018 (ABl. 2018 L 183, ABLEU Year 2018 L Heft 183) Page 23, which incorporated the GDPR into the EEA Agreement.

20. Data Breach

Requirement in a nutshell:
The SA has selected a platform that ensures its data recipients manage data breaches in conformance with the GDPR.

Relevant norms:
Art. 33, Art. 34, Art. 38(1), Art. 25 (1), Art. 12 (1), Art. 24 (1) GDPR **General Criteria**

20.1 Contact point

The SA has selected a platform that has defined a responsible contact point for data recipients to collect and assess potential data breach events.

The SA has selected a platform that has implemented processes to report data breaches to the designated contact point.

Option (a) data minimisation	Option (b) anonymisation
The SA has selected a platform that obliges its data recipients to notify the platform about any data breach.	

20.2 Processes to assess data breaches (Art. 33 (1)(1) GDPR)

The SA has selected a platform that obliges its data recipients to implement processes to identify occurring data beaches and assess whether it is likely to result in a (high) risk to the rights and freedoms of natural persons.

This process takes into account[32]:

- the type of breach;
- the nature, sensitivity, and volume of personal data;
- ease of identification of individuals;
- severity of consequences for individuals;
- special characteristics of the individual;
- special characteristics of the data controller;
- the number of affected individuals.

20.3 Notification and transparent information of the national supervisory authority (Art. 33 (1) GDPR)

The SA has selected a platform that obliges its data recipients to implement processes to inform the national supervisory authority and the CAB about an occurring data breach without undue delay, providing at least the following information (Art. 33 (3) GDPR):

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

[32] See Art. 29 Data Protection Working Party, Guideline on Personal data breach notification under Regulation 2016/679, WP250 rev.01, page 25-26.

- the name and contact details of the data protection officer or other contact point where more information can be obtained,
- the likely consequences of the personal data breach,
- the measure taken or proposed to be taken by the platform to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In case the data recipient or platform have not yet acquired all necessary information, it makes sure to at least notify the national supervisory authority about an occurring data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of the personal data breach. The notification contains reasons for the delay, in case the notification is not made within 72 hours.

20.4 Data Protection by Design

The SA has selected a platform that has specified a concept concerning the reaction on a data breach that contains at least the following items:

- the conditions under which the contact point is to be informed by any project member or employee of the suspicion that a data breach has occurred;
- who is to be informed when about what (see 20.2), including the DPO (Art. 38 (1) GDPR)[33];
- who is to be included in assessment and decision-making processes (see II.20.2);
- who is to inform the supervisory authority (see II.20.3);
- who is to inform the data subjects (see II.20.6);
- what is to be documented when and by whom (see II.20.5).

Proof / Evidence	Assessment methods
• Data breach reaction concept • Data breach DPO consultation concept • Data breach notification form • Data subject notification form	• Formal document check • Legal review • Interview with employee

20.5 Documentation

The SA has selected a platform that has implemented processes to document any personal data breaches, including all relevant facts relating to the personal data breach, its effects and the remedial action taken (Art. 33 (5) GDPR).

The SA has selected a platform that has implemented measures to document its reasoning for the decisions taken in response to a breach.

Proof / Evidence	Assessment methods
• Data breach assessment protocol • If applicable, data breach DPO consultation protocol • If applicable, data breach notification protocol	• Formal document check • Legal review

[33] See Art. 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 14.

20.6 Notification and transparent information of the data subject (Art. 34 (1) GDPR)

The SA has selected a platform that obliges its data recipients to implement measures to effectively inform data subjects about data breaches concerning them without undue delay.

The data recipient provides at least the following information (Art. 34 (3) in conjunction with Art. 33 (3)(b),(c),(d) GDPR):

- the name and contact details of the data protection officer or other contact point where more information can be obtained,
- the likely consequences of the personal data breach,
- the measure taken or proposed to be taken by the SA to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In case the data recipient has not yet acquired all necessary information, it makes sure to at least notify data subjects about an occurring data breach.

The information is provided to the data subject in a way consistent with the requirements of transparent information (see II.16. Transparency).

21. IT Security

Requirement in a nutshell:
The SA has selected a platform that ensures a level of security appropriate to the risks caused by the processing of personal data to fundamental rights of data subjects.

Relevant norms:
Art. 32, Art. 30 (1)(g), Art. 24 (1), Art. 5 (2) GDPR **General Criteria**

21.1 Processes to assess the risks to fundamental rights of the data subject

The SA has selected a platform that has implemented processes to assess the risks to fundamental rights of the data subject that result from the processing of personal data for the specified purposes (see 4. Purpose specification and limitation with respect to its processing operation) and by conducting the specified processing operations (see II.4. Purpose specification and limitation with respect to its processing operation) according to this scheme. For the implementation of such risk assessment, see 5. Mandatory data protection impact assessment.

The SA has selected a platform that has implemented processes to determine an appropriate level of security to mitigate these risks.

21.2 Data protection by design

The SA has selected a platform that has implemented effective technical and organisational measures to ensure a respective level of security, including

1. pseudonymisation and encryption of personal data;
2. limiting access to personal data and identifiers to qualified personnel by assigning tasks, roles, responsibilities, competencies and access rights to its employees,
3. introducing confidentiality requirements and non disclosure agreements to those employees
4. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
5. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident by providing backups;
6. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Proof / Evidence	Assessment methods
• IT security concept • Pseudo-/anonymisation concept • Synthetisation concept • Concept for access and entry restriction to buildings and rooms in which personal data is stored • Role and authorization concept for electronic data access with differentiation between read and write rights • Data storage concept • Restart & recovery concept	• Formal document check • Legal review • Audit (org.)

21.3 Documentation

The SA documents:

- all assessments and decisions performed for determining an appropriate level of security
- all technical and organisational measures implemented to ensure this level of security (Art. 30 (1)(g) GDPR)
- the performance and effectiveness of the implemented measures and processes.[34]

If the SA deviates from the state of the art (to the detriment of data subjects), it must document the reasons for doing so, especially referring to the cost of implementation.

Proof / Evidence	Assessment methods
• Pseudo-/anonymisation protocol • Synthetisation protocol • Confidentiality and non disclosure agreements • Employee data protection training certificates / protocols • Record of processing activities • Data access protocol • If applicable, restart & recovery protocol	• Formal document check • Legal review • Audit (org.)

21.4 Monitoring

The SA has implemented processes to test, assess and evaluate on a regular basis the effectiveness of the technical and organisational measures.[35]

The SA has implemented measures to take into account any changes of the following factors that are likely to affect the effectiveness of the processes described above:

- changes of risks or risk levels, e.g. due to new developments in the IT security field,
- changes of the scope, context and purposes of the processing activities,
- changes in the applicable regulatory framework
- and changes of the responsibilities and functions affecting the processing activities.

Proof / Evidence	Assessment methods
• Eventually updated concepts • Eventually updated documentation • Random sample after 1 year • Time stamps • Version history	• Formal document check • Legal review • Audit (org.)

[34] See BSI, ISMS.1 Sicherheitsmanagement, ISMS.1.A13 Dokumentation des Sicherheitsprozesses (S).
[35] See BSI, ISMS.1 Sicherheitsmanagement, ISMS.1.A11 Aufrechterhaltung der Informationssicherheit (S).