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 prediction systems in health care

HIIG DISCUSSION PAPER SERIES 2026-02

ABSTRACT

The present conformity assessment program was developed within the framework of the BMFTR-funded project "KI in der Pflege – Sturz, Delir, Medikation (KIP-SDM)" (AI in Nursing – Falls, Delirium, Medication). The primary aim of the project was to improve the quality of predicting fall events during treatment by using routinely collected patient or treatment data, and, in connection with this, to reduce the risk of fall events. The project examined how extensive clinical and nursing data sets can be used to train prediction models while at the same time protecting the interests and fundamental rights of patients and persons in need of care.

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 training prediction models, as well as the use of the trained models for the prediction and classification of risks and risk factors in a professional healthcare and nursing context. The program requires that the data be sufficiently anonymized and, where appropriate, synthetically generated before the models are trained. In addition, 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, Prediction systems, Clinical decision support systems, Health data, 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 prediction systems in health care. HIIG Discussion Paper Series 2026-02. 53 pages. https://doi.org/10.5281/zenodo.18442186.

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	7 February 2025	Nils Heinemann, Jörg Pohle
1.0	13 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 undertaking either an individual or consortium-based project with the objective of independently or jointly developing and training a predictive system for events or trends based on historical health and treatment data, to be implemented and operated with a project partner.

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 Purposes and processing operations

The ToE includes only processing operations conducted by the SA for purposes which can be subsumed under the following purpose categories referred to above:

2.1.1 Purpose 1: Training

The historical health and treatment data originating from a clinical institution are to be used to train a model capable of generating predictions for events or trends based on pattern recognition. To produce relevant training data, the historical health and treatment data will first be adequately anonymized and, if necessary, synthesized.

2.1.1.1 Data subjects

Data subjects are the patients of the clinical institution whose personal data are included in the datasets that are used, in anonymized form, as relevant training data for the purpose of model training.

2.1.1.2 Risks

Human dignity (Art. 1 ECFR)

The anonymization process preceding the training of the model entails 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 ECFR)

The anonymization process preceding the training of the model 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 ECFR)

The anonymization process preceding the training of the model entails 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 ECFR)

The anonymization process preceding the training of the model entails 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 anonymization process preceding the training of the model entails 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 anonymization process preceding the training of the model entails 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 anonymization process preceding the training of the model entails 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 anonymization process preceding the training of the model entails 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).

Further risks to fundamental rights

Next to these mentioned risks, the anonymization process preceding the training of the model may lead to further, yet undetermined risks to fundamental rights and freedoms, depending on the context, the social actors involved, the foreseeable downstream purposes as well as the means employed.

2.1.1.3 Benefits

Due to the technically and legally complex access to historical health and treatment data, the potential for training AI-based prediction systems has not yet been fully realised. The implementation of appropriate anonymization and synthesis procedures prior to training the prediction system now enables, for the first time, the data protection-compliant development of an AI-based prediction infrastructure, even across multiple institutions.

2.1.2 Purpose 2: Usage

At one consortium partner, the trained prediction model is to be used to analyze risk classification and related risk factors, with the results being directed to specially trained and qualified professionals. If the results prove to be accurate, concrete clinical or care-related action recommendations can be derived from

the predictions and implemented accordingly.

2.1.2.1 Data subjects

Data subjects are 1) patients of the clinical institution whose personal data are processed and used in the course of deploying the prediction system for medical and/or care-related activities.

Data subjects are 2) care professionals of the clinical institution whose personal data are collected, processed, and used in the course of deploying the prediction system for the documentation of medical and/or care-related activities, as well as for demonstrating the safe and legally compliant use of the system.

2.1.2.2 Risks

On the one hand, the prediction model itself can directly pose risks by making significantly poorer predictions for certain individuals with specific characteristics compared to others.

On the other hand, risks to the fundamental rights of data subjects may also arise indirectly from the users of the prediction model, who may misinterpret or improperly implement the recommended actions.

Human dignity (Art. 1 ECFR)

The use of the prediction model entails 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 ECFR)

The use of the prediction model 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 ECFR)

The use of the prediction model entails 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 ECFR)

The use of the prediction model entails 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 ECFR)

The use of the prediction model entails 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 use of the prediction model entails 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 use of the prediction model entails 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 use of the prediction model entails 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).

Fair and just working conditions (Art. 31 ECFR)

The use of the prediction model entails risks to the data subjects' fundamental right to fair and just working conditions under Article 31 of the EU Charter of Fundamental Rights (EU-CFR).

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

The use of the prediction model entails 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 use of the prediction model entails 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 use of the prediction model 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.

2.1.2.3 Benefits

The practical application enables more accurate predictions at a consistently high level. These improvements result, on the one hand, from fewer false-negative predictions, meaning fewer overlooked individuals, and, on the other hand, from fewer false-positive predictions, meaning fewer inappropriate interventions are undertaken.

2.2 No data transfer

Transfer of personal data to third countries according to Articles 44 ff. GDPR is not admissible under this scheme.

2.3 No automated decision making

By limiting the scope to the two purpose categories described above, processing operations that pursue automated individual decision making according to Article 22 GDPR cannot and must not fall under the scope of this scheme. The precondition that Article 22 GDPR does not apply to the scope of this scheme is thus already addressed by criteria 4 assessing purpose specification and limitation.

Automated decision-making in accordance with Article 22 of the GDPR through purely technical means is not intended for the purposes of processing and will not be applied in accordance with the principle of purpose limitation. A de facto automated adherence to decisions made by humans, meaning a consistently positive bias and uncritical trust in the system's decisions, is largely excluded through staff training and internal guidelines for the use of the decision system.

2.4 Higher requirements for some criteria

Finally, 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 for controllers or processors not established in the Union a representative, to maintain a record of processing activities and carry out a risk assessment that fulfils the requirements of a data protection impact assessment pursuant to Article 35 GDPR.

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

1. A data protection impact assessment (DPIA) pursuant to Article 35 GDPR must be carried out and documented.
2. A record of processing activities must be maintained that goes beyond the requirements of Article 30 GDPR for records of processing activities but is substantively necessary.
3. Appropriate measures must be taken in accordance with Article 22(3) GDPR to demonstrate that not only is there no intended automated decision-making in individual cases, but also no de facto (so-called automation bias).
4. When engaging a processor, the contract or other legal instrument between the controller and the processor must be concluded prior to the commencement of processing.

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 the processing of personal data on websites 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. Transparency
8. Data subject rights
9. Data minimisation
10. Storage limitation
11. Third country transfer
12. Data breach
13. IT-Security
14. Data protection by design

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 (and if applicable, a representative)

The SA has designated a DPO (irrespective of the size, legal structure or core activities of the company), 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 employees 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 employees with the GDPR,
- to cooperate with and to act as the contact point for the supervisory authority and the CAB.

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 business sector the SA operates in,
- 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 in the company 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 to its role as DPO (e.g. theft, physical, psychological or sexual harassment

[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.

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 joint controllers and all employees involved in training and deploying the model regarding their obligations under the GDPR,
- monitor compliance with the GDPR and other data protection regulations, as well as the strategies of the joint controllers for protecting personal data, including the assignment of responsibilities, raise awareness, and train of employees involved in the training and deployment of the model, 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 the training and deployment of the model.

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,
- access to key stakeholders (e.g., model developers, 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 easily and directly accessible to data subjects, supervisory authorities, the CAB and departments within the company and is able to receive, process and respond to requests within an appropriate time frame

[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.

(Article 38(4) GDPR).

Proof / Evidence	Assessment methods
• Internal DPO concept (including task & process descriptions, policies, organizational charts) • DPO contract and certificate of appointment • 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 project 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 company[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 project 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 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)	• Formal document check • Legal review (to clarify unclear terms)

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

process descriptions, policies, organizational charts, resources) • Disagreement / deviation case documentation with justifications	

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

[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 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 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 • The entirety of documented compliance to data protection regulation as defined	• 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.

in 2.1 • Random sample	

2.3 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

2.4 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	• Formal document check and legal review (to clarify unclear terms) • Audit (org): Interview with DPO

[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 3.7 and 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 7. 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 3.2 (see also: 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 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 Article 28 of the GDPR:

[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.

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 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
- to store the personal data only for the duration necessary to provide the service, at most for as

[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.

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

[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.

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 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 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. The purpose must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow compliance with the law can be assessed and data protection safeguard applied. For these reasons, a purpose that is vague or general will – without more detail – not meet the criteria of being 'specific'. The degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved.

In cases where different purposes exist from the beginning and different kinds of data are collected and processed simultaneously for these different purposes, the data protection requirements must be complied with separately for each purpose.[25]

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:

- Purpose 1 "Training": The historical health and treatment data originating from a clinical institution are to be used to train a model capable of generating predictions for events or trends based on pattern recognition. To produce relevant training data, the historical health and treatment data will first be adequately anonymized and, if necessary, synthesized.
- Purpose 2 "Usage": At one consortium partner, the trained prediction model is to be used to analyze risk classification and related risk factors, with the results being directed to specially trained and qualified professionals. If the results prove to be accurate, concrete clinical or care-related action recommendations can be derived from the predictions and implemented accordingly.

As the ToE includes only processing operations conducted by the SA for purposes which can be subsumed under the purpose categories defined above under Scope, 2.1, the respective purposes have to be specified here in such a way that the SA can show that these purposes can be subsumed under either Purpose 1 "Training" or Purpose 2 "Usage".

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

4.1.1 Proper purpose specification

The SA has implemented processes to properly specify the processing purposes 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 purposes 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 4.1.1).
These processes take into account:

- Any link between the purposes for which the personal data have been collected and the purposes 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 Article 9 GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 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 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	• Formal document check • Legal review (to clarify unclear terms)

• Data minimisation or anonymisation concept • List of specified processing purposes and sub-purposes	

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 purposes 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, comparing prediction precision, or backups.

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

4.3 Transparency

The SA has implemented measures to provide each data subject, in particular patients, with all necessary information on the processing purposes in a precise, transparent, comprehensible and easily accessible form in clear and understandable language.

Proof / Evidence	Assessment methods
• Information sheet in various languages • Verbal patient instruction	• Formal document check • Readability assessment

4.4 Documentation

The SA documents:

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

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

(text, tables)	

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 purposes of the processing;
    2. assess the necessity and proportionality of the processing operations in relation to the 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 the project. The risk assessment covers at least the risks to the fundamental rights and freedoms referred to in sections I. 2.1.1.2 and 2.1.2.2 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 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 purposes;
- an assessment of the risks to the fundamental rights and freedoms of data subjects referred to in section 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 assessing the efficacy and effectiveness of the measures envisaged to address the risks • Literature review wrt the state of the art of the measures 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' 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' 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

Specific criteria

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 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 purposes, 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 purposes specified in chapter 1 of this scheme.

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.

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

7. Transparency

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

Relevant legal norms:
Art. 12, Art. 13, Art. 5 (1)(a), Art. 5 (2), Art. 24 (1) GDPR **Specific criteria**

7.1 Information according to Art. 14 GDPR

For the training of the prediction model, where personal data have not been obtained directly from the data subject, the SA is not obliged to provide the data subject with in-depth information, for this would prove impossible or involve a disproportionate effort according to Art. 14 (5)(b) GDPR.
In this stance, the SA has implemented processes to protect the data subject's rights and freedoms and legitimate interests, including providing public information, e.g. on the project's website, about:

- the identity and the contact details of the SA;
- 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.

7.2 Information according to Art. 13 GDPR

For the usage of the prediction model, where personal data have been collected directly from the data subject, the SA has implemented processes to provide the data subject at the moment of data collection with the following information:

- the identity and the contact details of the SA;
- if applicable, the identity and the contact details of the controller's representative;
- the purposes of the processing for which the personal data are intended;
- the consent of the data subjects as the legal basis for the processing according to the treatment contract;
- the recipients or categories of recipients of the personal data,
- the storage duration, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to personal data;
- the existence of the right to rectification or erasure of personal data;
- the existence of the right to restriction of processing personal data;
- the existence of the right to object to processing;
- the existence of the right to data portability;
- if applicable, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the existence of the right to lodge a complaint with a supervisory authority;
- if applicable, whether the data subject is obliged to provide the personal data and information

about the possible consequences of failure to provide such data;
- the fact that automated decision-making in accordance with Article 22 of the GDPR through purely technical means is not intended for the purposes of processing and will not be applied in accordance with the principle of purpose limitation;
- 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 purposes (see 5. DPIA).

If the SA collects and processes personal data for additional purposes for which it does not receive certification under this scheme, the **SA clearly and visibly separates and demarcates the certified purposes from non-certified purposes** when acquiring the users' consent for these purposes.

Remark:
In case the controller intends to further process the personal data for a purpose other than for which it was collected, the controller provides the data subject with all relevant information on that other purpose as referred to above. This informational duty applies irrespective of the legality of such purpose changes.

However, all purpose changes of this kind already fall out of scope of this scheme.

7.3 Data protection by design (transparent information)

The SA has implemented measures to provide each data subject, in particular patients, with all necessary information according to Art. 13 GDPR (as listed above).

Proof / Evidence	Assessment methods
• Data protection policy • Public website in various languages with all information listed in chapter 7.1 • Detailed legal information sheet in various languages with all necessary information according to Art. 13 GDPR (as listed in chapter 7.2) • Detailed verbal patient instruction containing all necessary information according to Art. 13 GDPR (as listed in chapter 7.2)	• Formal document check • Legal review • Readability assessment • Audit (org)

7.4 Documentation

The SA 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 via sheets (text, tables) and	• Formal document check • Legal review • Audit (org): interview with employees

time of information • Documentation of provided information via verbal patient instruction (text, tables) and time of information	

7.5 Monitoring

The SA 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

8. Data subject rights

Requirement in a nutshell:
The SA guarantees 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**

8.1 Facilitation of data subject rights

The SA has implemented measures to ensure that it is as convenient as possible for the data subjects to exercise their rights.
The SA provides multiple ways for data subjects to exercise their rights, both analog and digital, such as:

- 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 project's or partner institutions' 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

8.2 Right of access (Art. 15 GDPR)

The SA has implemented measures to provide data subjects with confirmation as to whether or not personal data concerning them are being processed upon their request. Where that is the case, the SA 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;

8.3 Right to rectification (Art. 16 GDPR)

The SA has implemented measures to rectify inaccurate personal data concerning data subjects without undue delay upon request of the data subject. The SA 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.

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

The SA has implemented measures to erase personal data concerning the data subject without undue delay upon request of the data subject. In particular, the SA erases 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).

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

The SA has implemented measures to restrict 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.

8.6 Right to object (Art. 21 GDPR)

If the processing of personal data is based on Art. 6 para. 1 lit. e) or f) GDPR, the SA has implemented measures to stop 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 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.

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

The SA has implemented measures to ensure the data subject's right to withdraw their consent at any time. The SA 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 informs the data subject thereof. The SA ensures that it is as easy to withdraw as to give consent.

9. Data minimisation

Requirement in a nutshell:
The SA only processes personal data to an extent necessary to achieve the specific purposes.

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**

9.1 Processes to assess the data minimisation principle

The SA has implemented measures to assess whether it only processes personal data that is adequate, relevant and limited to what is necessary for achieving the intended specific purposes (see 4. Purpose specification and limitation with respect to its processing operation).[26]
This assessment includes:

- an evaluation of whether processing personal data is necessary in the first place. In this assessment, the SA verifies whether the specific purposes can be achieved by processing less, only aggregated or no personal data at all.[27]
- an evaluation to what degree the data subject needs to be identifiable in order to achieve the specific purposes. In this assessment, the SA assesses whether it can achieve the intended purposes also by only processing pseudonymised or anonymised data and if so, determines the earliest point in time when pseudonymisation or anonymising personal data is feasible.[28] (see also 9.2 Data protection by design)

9.2 Data protection by design

The SA has implemented effective measures to delete all identifiers and/or raw data as soon as identification is no longer needed and/or the processing of aggregated data is sufficient.[29]

The SA has 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).

The SA has implemented effective measures to pseudonymise and/or anonymise datasets, using state of the art methods.[30]

Proof / Evidence	Assessment methods

• Data flow diagram
• Data minimisation concept, incl.
  ○ access and authorisation concept
  ○ pseudo-/anonymisation concept
  ○ synthetic data concept
• On request: access to IT system
	• Formal document check
	• Legal and technical review
	• Audit (org): interview with DPO

[26] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 73.
[27] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 74.
[28] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 75.
[29] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 75.
[30] See EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 21.

9.3 Documentation

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

Proof / Evidence	Assessment methods
• Deletion protocol • Access and authorisation protocol • Pseudo-/anonymisation protocol • Synthetisation protocol	• Formal document check • Legal and technical review • Audit (org): Interview with DPO

9.4 Monitoring

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

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

10. Storage limitation

Requirement in a nutshell:
Personal data is only stored 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[31]

General criteria

10.1 Retention period

The SA 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 specified clearly and transparently the retention period or the deletion conditions.

The SA has implemented mechanisms to ensure that the data used for the training is deleted from the project by the end of the training at the latest.

10.2 Erasure of personal data

The SA 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 for configuring an automated deletion mechanism; and
- how the deletion will be documented.

(see alternatively below: 10.3 Anonymisation of personal data)

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

10.3 Anonymisation of personal data

The SA has implemented measures to ensure that the personal data is pseudonymised or anonymised at the earliest possible date and according to the state of the art, and the pseudonymisation or anonymisation is documented.

The SA has specified clearly and transparently:
- when the data will be pseudonymised or anonymised;
- what pseudonymisation or anonymisation methods will be used;
- what metrics and/or threshold values will be used to assess the quality of the achieved

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

pseudonymisation or anonymisation;
- who is responsible for pseudonymising or anonymising the data; and
- how the pseudonymisation or anonymisation will be documented.

The SA has implemented measures to ensure that the synthetisation of data is done with an adequate generator model trained on pseudonymised or anonymised data, both according to the state of the art, and the synthetisation is documented.

The SA has specified clearly and transparently:
- with what methods the generator model is trained;
- how the quality of the generator model is assessed;
- what methods, metrics and/or threshold values will be used to assess the quality of the achieved anonymity of the synthetic data;
- who is responsible for model training and data synthetisation; and
- how the model training and data synthetisation will be documented.

(see alternatively above: 10.2 Erasure of personal data)

Proof / Evidence	Assessment methods
• Pseudo-/anonymisation concept • Synthetisation concept • Pseudo-/anonymisation protocol • Synthetisation protocol	• Formal document check • Legal review

11. 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 does not transmit personal data to third countries or international organisations.

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.[32]

Any country that is not a member of the European Union (EU) or European Economic Area (EEA) is regarded as a third country.[33]

[32] See Recital 48 (2) GDPR.
[33] 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.

12. Data Breach

Requirement in a nutshell:
The SA manages 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**

12.1 Contact point

The SA has defined a responsible contact point to collect and assess potential data breach events.
The SA has implemented processes to report data breaches to the designated contact point.

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

The SA has implemented 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[34]:

- 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.

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

The SA has implemented 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,
- 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 SA has 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.

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

12.4 Data Protection by Design

The SA has implemented effective measures to confirm with the requirements imposed in 12.1 – 12.3.
The SA 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 12.2), including the DPO (Art. 38 (1) GDPR)[35];
- who is to be included in assessment and decision-making processes (see 12.2);
- who is to inform the supervisory authority (see 12.3);
- who is to inform the data subjects (see 12.6);
- what is to be documented when and by whom (see 12.5).

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

12.5 Documentation

The SA 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 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

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

The SA has implemented measures to effectively inform data subjects about data breaches concerning them without undue delay.

The SA 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,

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

including, where appropriate, measures to mitigate its possible adverse effects.

In case the SA 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 7. Transparency).

13. IT Security

Requirement in a nutshell:
The SA 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**

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

The SA 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 4. Purpose specification and limitation with respect to its processing operation) according to this scheme. For the implementation of such risk assessment (see 5. Data protection (risk and) impact assessment).

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

13.2 Data protection by design

The SA 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.)

13.3 Documentation

The SA documents (see 2. Documentation)

- 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.[36]

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.)

13.4 Monitoring

The SA has implemented processes to test, assess and evaluate on a regular basis the effectiveness of the technical and organisational measures.[37]

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.)

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

14. Data protection by design

Requirement in a nutshell:
The SA 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 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[38]. All remaining risks must also be effectively controlled with technical and organisational measures.

The SA 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	• Formal document check

[38] see I. Scope.

operations that are not covered by the DPIA • If applicable, risk assessments with associated protection measures	• Interview with DPO