# Trusted Site Data Privacy

## Criteria Catalogue for Inspecting the Conformity of an IT Solution with the European General Data Protection Regulation

## Version 2.16 from 27.01.2026

***public version***

**Criteria Catalogue Version**: 2.16

**Contact:**
TÜV NORD CERT GmbH
Certification authority
Am TÜV 1
45307 Essen, Germany

# Table of contents

# 1. Introduction and general information

## 1.1 Focus of content

This document contains the Trusted Site Data Privacy certification criteria for a national certification scheme for Germany in accordance with Article 42 para. 5 of the GDPR.

This criteria catalogue describes requirements for processing operations that are carried out in processes or with the help of several processes/systems in a function as Controller or Processor. The processing operations under consideration are referred to as

**Information Processing Services (IPS).**

For providing IPS, both software and combined software/hardware solutions may be employed.

Apart from the specific IPS itself, also its basic conception of the operational concept is considered under the criteria below. This conception is deemed an intrinsic part of the IPS since it may describe any important prerequisites for the data protection-compliant handling of the technical components of the IPS. Therefore, the documentation of the IPS and of the specifications for its operation plays an essential role in the assessment.

Overall, with regard to the IPS, the following components are part of the inspection object:

A The IPS in its technical design as a combination of
- A1 Hardware components,
- A2 Software components,
- A3 Network components, as well as
- A3 Processes supported by these components,

B The documentation of the IPS with the description of:
- B1 Properties of the IPS (process documentation functional/technical),
- B2 Instructions for use of the IPS (user documentation functional/technical),
- B3 If applicable, separate operational concept (if not included in B1/B2),
- B4 Change information.

C Documents and other information provided for use with the IPS:
- C1 Forms,
- C2 Information texts (e.g. consent texts),
- C3 Web pages,
- C4 Contract texts (e.g. contract for commissioned data processing).

All components of the IVS that are not part of the evaluation subject are not included in the evaluation and are out of scope in the context of certification. The IPS is intended to support data protection and compliance to it by users and make controllable deviating practices contradicting data protection, though not being able to completely prevent them.

### Limitation of the validity of this criteria catalogue

This criteria catalogue is based on the following assumptions/restrictions when describing these requirements:

1. The processing activities of the IPS concern personal data.
2. The IPS can be clearly delineated as a solution with its functionalities.
3. Personal data relating to criminal convictions and offences under Art. 10 GDPR are not processed.

4. Data processing does not take place in the context of employment (Art. 88 GDPR).
5. The certification cannot be used as an instrument for the transfer of personal data to a third country or an international organisation pursuant to Art. 46 para. 2 lit. f GDPR.
6. Certification for companies that do not have an establishment in the EEA, is not covered by the criteria catalogue.
7. The following applies to the certification of a processor under this certification scheme: Certification applicants under this certification scheme must be processors. This includes processors who are directly entrusted with the processing of personal data by a controller as well as sub-processors being engaged by a processor in accordance with Art. 28 para. 2 and para. 4 GDPR. The certification of a processor under this certification scheme does not automatically imply certification of any sub-processors engaged by the processor. However, sub-processors can also apply for certification themselves, which would be carried out in a separate and independent procedure."
8. In accordance with Art. 42 para. 1 GDPR, only processing operations can be certified with this criteria catalogue. In contrast to other certification procedures/options, this is a data protection-specific certification procedure in which the conformity of the processing operations with the requirements of the GDPR is determined. It is not purely a product or service certification. Furthermore, neither companies nor pure data protection management systems or data protection officers are certified.
9. No joint controllership pursuant to Article 26 of the GDPR can be certified on the basis of this criteria catalog.

## 1.2 Notes on the presentation of the program requirements

*Criterion number* | Definition of requirements

| | |
|---|---|
| DP01.01 | **A) Controller and Processor**<br>The IPS is **documented to a sufficient extent** and is sufficiently up to date. In particular<br>1. A technical process description<br>▪ Description of the IPS functions and the associated modalities. Main target group: (Potential) users as well as<br>2. a technical process description<br>▪ Description of the technical requirements and features of the IPS. Main target group: (Potential) system administrators and technically experienced users.<br>is provided.<br>Users of the IPS will additionally be provided with<br>1. a specialised user documentation,<br>▪ Description of the technical use of the IPS. Main target group: Users.<br>2. a technical operating/system documentation<br>▪ Description of the maintenance and management of the IPS, including the necessary technical background information on its use. Main target group: IPS system administrators, technically experienced users.<br>In the context of service updates and changes, the users of the service receive<br>1. Change information (release notes) |

| | |
|---|---|
| | ▪ Description of the changes to the IPS as part of new versions / releases. Main target group: Users and system administrators.<br>The processor must communicate changes to the IPS, such as new functions, improvements, etc., to the controller with within at least 14 days before the intended implementation. Appropriate communication channels must be established. The controller must be provided with all the information necessary to assess the impact of the changes on the processing activities, in particular a specific description of the intended changes, a complete list of security updates, release date. |
| *Type of determination* | ***DP** Verification of the existence of the information of numbers 1.-6. Evaluation of the quality, timeliness and completeness of the documentation provided by the evaluator.* |
| *Proof* | *Provision of the individual documents according to 1.-5. and presentation of where and in what form the respective information is contained. Furthermore, information on how the information is provided and how operators and persons affected by the IPS can obtain an overview of the documentation.* |
| **Customer description** | **The implementation of the respective test criteria is to be described in a clear and concise manner. Simply linking documents is not admissible. Page references to the supporting documents are required in the description for the core statements listed.** |
| **Designation of existing proof** | **All supporting documents are managed documents with version information, creation date and change history.** |

### *Criterion number*

The criterion number is made up of the catalogue abbreviation (here DP for data protection), the number of the section (here **DP01**) and the number of the individual criterion (here 01).

### *Definition of requirements*

The individual requirements reflect verifiable specifications relating to characteristics of the IPS or its basic conception of the operational concept. Within the specifications of requirements, a differentiation is made between Controller and Processor. Insofar as the body to be certified is a Controller, the requirements for Controllers, apply accordingly.

If the Processor service is to be certified, the requirements placed on Processors must be fulfilled accordingly.

The evaluator must be able to answer these formulations with "yes" or "no". In the case of a "yes", this statement must be linked to evidence, i.e. it must be verifiably substantiated.

The wording is strongly based on the text of the GDPR, but is usually formulated more simply, as the focus is on a clear verification statement. In case of doubt, the exact wording in the referenced article of the GDPR must therefore be considered.

### *Type of determination*

These test instructions describe specific verification procedures that are to be applied with regard to the criterion. They refer to the procedures listed in the certification scheme[1] under "Investigation methods":

**DP_General document** review
**DP_Ttechnical** document review

[1] GDPR certification programme of TÜVIT

| | |
|---|---|
| **DP_M** | Methodical document review |
| **DP_J** | Legal document review |
| **AN** | analysis |
| **AU** | Audit of the organisation |
| **IN** | Inspection of the evaluation object |
| **AU** | Evaluation of investigations |

*Evaluation note*

Where necessary and appropriate, individual evaluation requirements are broken down and specific verification procedures are described in detail in the evaluation note. This substantiates the individual requirements and at the same time ensures a uniform assessment of the evaluators. The evaluation notes must be observed.

*Proof*

Evidence proves the implementation of the criterion. It must be noted that the use of the word "can" in no way implies that evidence is optional at this point. Rather, it expresses the fact that alternative forms of evidence are possible/acceptable. In principle, the acceptance of evidence is in the judgment of the evaluator. Individual components of the evaluation object are reviewed as part of an on-site visit (audit).

*Vote*

The vote is to be completed by the evaluator and refers to the assessment of the fulfilment of the criterion under review.

## 1.3 Notes on the criteria catalogue

This criteria catalogue will become part of the *Trusted Site Data Privacy Test* Report, Version 2.0.

## 1.4 Abbreviations used

| | |
|---|---|
| Par. | Paragraph |
| Art. | Article of the GDPR |
| BDSG | Bundesdatenschutzgesetz (Federal Data Protection Act) |
| BetrVG | Betriebsverfassungsgesetz |
| BGBl. | Federal Law Gazette |
| SCPD | Special categories of personal data [GDPR] Art. 9. (“sensitive data”) |
| BMV-Ä | Bundesmantelvertrag-Ärzte |
| BSI | Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) |
| ex. | example |
| CMEK | Customer Managed Encryption Keys |
| GDPR | General Data Protection Regulation |
| GenDG | Genetic Diagnostics Act |
| DSK | Data Protection Conference |
| EDPB | European Data Protection Board |
| ENISA | European Union Agency for Cybersecurity |
| ff. | following |

| | |
|---|---|
| IMSI | International Mobile Subscriber Identity |
| ISMS | Information Security Management System |
| IPS | Information processing service (= evaluation object) |
| lit. | litera |
| PD | Personal data |
| PDP | Personal Data processing |
| marginal no. | Marginal number |
| SDM | standard data protection model |
| SGB | Social Code |
| ToM | Technical and organisational measures |
| TDDDG | Telecommunications Digital Services Data Protection Act |
| TVG | Collective Labour Agreement Act |
| cf. | compare |

## 1.5 References to laws, regulations and standards

In detail, the individual criteria topics/chapters refer to the following legislation, judgments and resolutions / recommendations of the supervisory authorities (DSK, EDPB etc.):

| | |
|---|---|
| [GDPR] | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| [BDSG] | Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as amended by Article 7 of the Act of 6 May 2024 (Federal Law Gazette 2024 I Nr. 149) |
| [TDDDG] | Telecommunications Digital Services Data Protection Act of 23 June 2021 (Federal Law Gazette I p. 1982), last amended by Article 44 of the Act of 12. Juli 2024 ( (Federal Law Gazette 2024 I Nr. 234) |
| [FÜ.B] | OKKSA e. V.: Catalogue of requirements for specialist programmes in public administration Sub-section: Interdisciplinary service requirements (OKKSA FÜ.B criteria) |
| [DSK_17067] | Requirements for data protection certification programmes<br>Data protection test criteria, test systems and test methods for the adaptation and application of the technical standard DIN EN ISO/IEC 17067 (programme type 6) version 2.0 dated 21.06.2022 |
| [SDM] | The standard data protection model<br>A method for data protection consulting and auditing based on standardised assurance objectives<br>Version 3.1 dated 14/05/2024 |
| [GL2020-07] | Guidelines of the European Data Protection Board 07/2020 on the concepts of Controller and Processor in the GDPR Version 2 |
| [GL2019-04] | Guidelines 2019-04 on Article 25 Data protection by design and by default Version 2 |

| | |
|---|---|
| [BSI-TR-02102-1] | Cryptographic methods: Recommendations and Key Lengths, Part 1 as of 24/03/2021 |
| [BSI-TR-02102-2] | Cryptographic procedures: Use of Transport Layer Security (TLS) Part 2 Version 2021-01 |
| [BSI-200-3] | BSI Standard 200-3 "Risk analysis on the basis of IT baseline protection" |
| [DIN ISO 31000] | Risk management |
| [ISO/IEC 27005] | Information security, cybersecurity and privacy protection — Guidance on managing information security risks |
| [DIN EN ISO 14971] | Medical devices — Application of risk management to medical devices |

## 1.6 evaluation object

The evaluation object is the concrete object of an evaluation. The evaluation object is data processing by means of information processing services (IPS). IPS can only be processing operations pursuant to Art. 42 para. 1 GDPR. Both software and combined software/hardware solutions can be used to provide the IPS.

In addition to the IPS itself, the following criteria also consider the operational concept of the evaluation object itself. This is seen as an intrinsic part of the IPS, as it may describe important prerequisites for the data protection-compliant handling of the technical components of the IPS. Accordingly, the documentation of the IPS and its operational specifications play a key role in the assessment.

Overall, the following components are part of the evaluation object with regard to the IPS:

A The IPS in its technical form as a combination of
A1 hardware,
A2 software and
A3 network components as well as
A4 processes supported by these components.

B The documentation of the IPS with the description:
B1 Properties of the IPS (functional/technical process documentation),

B2 Instructions for use of the IPS (functional/technical user documentation),

B3 separate deployment concept/operating concept (if not included in B1/B2),
B4 Change information .

C Documents and other Information provided for use with the IPS:

C1Forms,
C2 Information texts (e.g. consent texts),
C3 Internet pages,
C4 Contract texts (e.g. contract for Processor).

In order to determine the evaluation object, the applicant must carry out a complete data flow analysis of the IPS, taking into account all actors involved in the processing of personal data, e.g. Processors, sub-processors, joint controllers, and then prepare and submit a qualified representation of the entire processing process organized by phase, including a description of the respective actor and role model (actors, roles, relationships) for each processing phase. The representation can either be in the form of a graphic representation (e.g. using standardized representations such as Business Process Modelling (BPM) or Unified Modelling Language (UML)) or in text form.

The qualified representation of the processing process must map the complete life cycle of the processing of personal data within the IPS.
The definition of "processing" in Art. 4 para. 2 GDPR does not exhaustively list individual processing operations.

In addition, it must be determined and documented which data processing steps are to be assigned to the applicant's extended area of responsibility. It must also be clearly stated how the access options of the Controller and Processor are organized in the respective data processes. All data processing steps and relevant interfaces must be fully documented. The applicant must also identify the processing operations to be certified, which are the subject of the evaluation, so that the respective evaluation object can then be determined in consultation with the certification body and considering the information in accordance with 1.7 to 1.17.

The applicant must provide detailed information in accordance with 1.7 to 1.17 for the delimitation of the evaluation object before the start of the evaluation procedure. Based on this information, the evaluation object is then determined and documented accordingly in the Trusted Site Data Privacy Evaluation Report.

## 1.7 Designation of the evaluation object

| | |
|---|---|
| | The evaluation object can be a process or processing in a product, a system or within an infrastructure that processes personal data. The evaluation object must have a name and a version number (or date). If possible, the version must not change during the check. The certificate is issued for the tested version in the tested operating environment, if applicable. The name of the evaluation object can still be changed until the certification is finalised. |

### 1.7.1. Name and address of the applicant

| | |
|---|---|
| | Please state the name and address of the applicant. |

### 1.7.2. Processing operations in the context of the evaluation object

| | |
|---|---|
| | Description of which processing operations are covered by the evaluation object. |

### 1.7.3. Purposes of the processing operations in the context of the evaluation object

| | |
|---|---|
| | Description of the purposes which are covered by the respective processing operations and why these processing operations are necessary to achieve the purpose. |

### 1.7.4. Operating conditions

| | |
|---|---|
| | Presentation of the IT landscape in which the evaluation object is used, in which other processes it is integrated, use of encryption, on which operating systems it runs, etc. |

### 1.7.5. Agencies involved

| | |
|---|---|
| | Internal and external bodies relevant to the evaluation object (departments, Group companies, cooperation partners, computer centre). |

### 1.7.6. Recipients or categories of recipients

| | |
|---|---|
| | Recipients or categories of recipients of personal data relevant to evaluation object. |

### 1.7.7. Applicant

| | |
|---|---|
| | The company name, including address and legal form, must be provided. Furthermore, it must be stated whether the applicant is acting as a controller in accordance with Art. 4 No. 7 GDPR or as a processor in accordance with Art. 4 No. 8 GDPR. |

### 1.7.8. Use of processors or sub-processors by the applicant

| | |
|---|---|
| | If the applicant is acting as controller: Processors and sub-processors pursuant to Art. 4 No. 8 GDPR which are relevant for the evaluation object for each processing operation must be listed<br>If the applicant is acting as processor: sub-processors pursuant to Art. 4 No. 8 GDPR which are relevant for the evaluation object for each processing operation must be listed |

### 1.7.9. Transfer of personal data to third countries or international organisations

| | |
|---|---|
| | Description of whether personal data is transferred to third countries or international organisations with regard to the processing operations of the evaluation object.<br>All transfers must be recorded, including individual support, maintenance and care access and also possible extraterritorial access, e.g. due to business activities, as well as onward transfers by Processors. |

## 1.8 Description of the evaluation object

### 1.8.1. Architecture of the evaluation object and purpose of the (sub)components

| | |
|---|---|
| | Description of the main and sub-components and their purpose in the overall context.<br>The respective parties involved, e.g. customers, users, administrators, etc., must also be named.<br>A technical description that must be understood by data protection and IT lawyers must be provided here and in the following subsections. The aim is to provide an overview that also enables IT specialists to request more detailed information or documents for the security-related investigation. |

### 1.8.2. Flow of data between the components of the evaluation object

| | |
|---|---|
| | Presentation of the flow of data between the main and sub-components of the evaluation object, stating the data types and the parties involved. |

### 1.8.3. Delimitation of the evaluation object

| | |
|---|---|
| | It is essential for the audit to determine which components or interfaces (at the boundary to other procedures or systems) are to be included or not included in the audit (with an explanation of why they are to be included or not included, especially if the boundary is not clear from the architecture or purpose of the evaluation object). |

### 1.8.4. Processes and functionalities

| | |
|---|---|
| | Description of the individual processes and "functionalities" e.g. process registration for web applications, detailed description of workflows. |

### 1.8.5. Presentation of all processing activities within the evaluation object

| | |
|---|---|
| | Description also with regard to the responsibility of all processing activities organised by phase and the respective actor and role model (actors, roles, relationships) for each processing phase. |

## 1.9 Groups of data subjects, type of the personal data processed, origin of the data, purpose of their collection, processing, use

Depending on the evaluation object, the resulting structure of this chapter may differ, e.g. breakdown according to interfaces. The information must be as detailed as possible. Mere statements

such as “Customer data for customer care” or “Address data” are not sufficient; sufficient would be, for instance: “Date of birth (day, month, year) for age verification” or “Customer address (street, house number, address suffix, postcode, city, state) for brochure mailing”.

### 1.9.1. Affected groups

| | |
|---|---|
| | Here, indication of the groups of persons affected by data processing is required. |

### 1.9.2. Personal data

| | |
|---|---|
| | Data which the evaluation object aims to process, e.g. data subject data (breakdown from database).<br>It must be indicated which data<br>a) Are special categories of personal data pursuant to Art. 9 GDPR<br>b) relate to children within the meaning of the GDPR. |
| | *The restriction on the validity of the criteria catalogue regarding the processing of personal data relating to criminal convictions and offenses under Article 10 of the GDPR must be observed.* |

### 1.9.3. Origin of data

| | |
|---|---|
| | Here, indication of the source of the personal data is required. |

### 1.9.4. Purpose of processing

| | |
|---|---|
| | A clear statement of the purpose(s) is required for the personal data or category of data processed. |

### 1.9.5. Legal basis for the processing of personal data

| | |
|---|---|
| | Presentation and, where applicable, explanation of the legal basis for the processing of personal data in the (sub)components and in relation to the transmission of data and data types. |

## 1.10 Information technology equipment, including installation sites and operations

| | |
|---|---|
| | Here, the information technology equipment used for the evaluation object, including installation sites and operations, need to be identified. |

### 1.11 Service and steps taken for commissioning

| | |
|---|---|
| | Here, indication of the services used for the evaluation object and the steps taken for commissioning is required. |

### 1.12 Network plan

| | |
|---|---|
| | For networked information technology equipment, the physical and logical connections to other information technology devices must be shown. |

### 1.13 Interfaces

| | |
|---|---|
| | Of particular importance to the verification are the interfaces where data enters the system/process, is transferred within it from one (main) component to another one and leaves the system/process. Here, all interfaces, whether electronic or in the form of manual input or receipt of paper documents, need to be listed and described (which data fields, for what purpose, in what way). Additionally, security aspects are to be listed here, e.g. SSL encryption, registered letter, etc. It must be noted that administrator access is also deemed an interface. |

### 1.14 Import of data / input interface/s

| | |
|---|---|
| | Explanation of the import of data via possible input interfaces. |

### 1.15 Internal interfaces

| | |
|---|---|
| | The internal interfaces must be indicated here. |

### 1.16 Data transmission, output interface(s)

| | |
|---|---|
| | Transmission in the sense of data transmissions and within the scope of commissioned data processing. |

### 1.17 Access authorisations for PD

| | |
|---|---|
| | Indication of who/which group of persons is authorised to has access to PD, e.g. administrators of the company. |

# 2. Evaluation criteria

## DP01 Process documentation

The process documentation plays a prominent role in the assessment of IPS and its scenarios of use in the context of the GDPR. Whereas parts of the process documentation, which describe, in particular, its use, play a role in various criteria of this catalogue, basic requirements for the documentation are listed below, which are a prerequisite for the clear description and data protection-compliant use of the IPS.

[GDPR] Art. 24 para. 1

| | |
|---|---|
| DP01.01 | **Controller and Processor**<br>The IPS is **documented** and is up to date. In particular<br>1. A technical process description<br>▪ Description of the IPS functions and the associated modalities. Main target group: (Potential) users as well as<br>2. a technical process description<br>▪ Description of the technical requirements and features of the IPS. Main target group: (Potential) system administrators and technically experienced users.<br>is provided.<br>Users of the IPS will additionally be provided with<br>1. a specialised user documentation,<br>▪ Description of the technical use of the IPS. Main target group: Users.<br>2. a technical operating/system documentation<br>▪ Description of the maintenance and management of the IPS, including the necessary technical background information on its use. Main target group: IPS system administrators, technically experienced users.<br><br>In the context of service updates and changes, the users of the service receive<br>1. Change information (release notes)<br>▪ Description of the changes to the IPS as part of new versions / releases. Main target group: Users and system administrators.<br>The processor must communicate changes to the IPS, such as new functions, , improvements, etc., to the controller within at least 14 days before the intended implementation. Appropriate communication channels must be established. The controller must be provided with all the information necessary to assess the impact of the changes on the processing activities, in particular a specific description of the intended changes, a complete list of security updates, release date. |

[GDPR] Art. 12 para. 1

| | |
|---|---|
| **DP01.02** | **Controller and Processor**<br>All parts of the IPS documentation supplied to data subjects are available in German.<br>The specification of the individual requirements can be found in the evaluation note. |

[GDPR] Art. 24 para. 1

| | |
|---|---|
| **DP01.03** | **Controller and Processor**<br>The **technical operating documentation / system documentation** supports the user in the data protection-compliant use of the IPS by specifying:<br>1. technical and, if applicable, organizational requirements for the operation of the service, e.g.<br>▪ Need for a specific system environment,<br>▪ Necessity of certain additional components in the context of the usable functions,<br>▪ Necessity of instructions / training<br>2. limits on the usability of the service, e.g.<br>▪ Number of personal data records that can be recorded,<br>▪ Maximum log retention time for technical reasons,<br>▪ Guaranteed maximum service failure rate for 24/7 operation.<br>3. specifications for setting up the access management of the service, e.g.<br>▪ Information on which types of user roles are required to use the service,<br>▪ Instructions for setting up user administration,<br>▪ Recommendations for setting up access separation between users in accordance with data protection regulations.<br>4. requirements for the use of the security technologies used in IPS, e.g.<br>▪ Information about the encryption technologies used,<br>▪ Information about the signature components used,<br>▪ Information about the type of user authentication.<br>5. possible risks to the protection of the processed personal data resulting from the use of the IPS, e.g.<br>▪ risk of not updating software components,<br>▪ Risk of breaching access barriers,<br>▪ Risk of Third Party data collection. |

[GDPR] Art. 24 para. 1, **DP07.01, DP09.04**

| | |
|---|---|
| **DP01.04** | **Controller and Processor**<br>The **change documentation** provided with the service contains<br>1. a complete list of the changes relevant to the service functionality and its technical operating conditions,<br>2. per change<br>▪ a description of the change made,<br>▪ if necessary, measures taken by the user that are required in the context of the service change,<br>▪ if applicable, information on application modalities (e.g. modules used) for which this change is relevant,<br>▪ recognisability of service version or date from which this change was introduced. |

## DP02 Principles relating to processing

[GDPR] Art. 5 para. 1 lit. a

| | |
|---|---|
| DP02.01 | **Controller**<br>Personal data must be processed in a manner that is understandable to the data subjects (**principle of transparency**).<br>All information and notifications relating to the processing of personal data are made easily accessible to the data subject in clear and simple language, cf. DP06.01. In particular, the following is ensured:<br>• The data protection information is clearly separated from other information that does not relate to data protection, e.g. contractual provisions, general terms and conditions of use<br>• The data protection information is understandable for a typical member of the target audience (taking into account the level of understanding of the persons concerned).<br>• It is immediately apparent to the data subject where and how they can access the data protection information (easy accessibility)<br>• If the controller's target audience is children or the goods/services are used by children in particular, the choice of words, tone and style of language is adapted to the child target group<br>• The information provided includes the details specified in Art. 13 or 14 GDPR, see DP06.04 and DP06.05, so that the data subject can determine the scope and consequences of the processing.<br>• The controller actively provides the information in accordance with Art. 13 and 14 GDPR to the data subjects or directs the data subjects directly to the place where the information is available<br>• The data subject has permanent access to the information in accordance with Art. 13 and 14 GDPR<br>• The controller reminds the data subject at regular intervals (at least annually) of the data protection declaration/information and where it can be found<br>• A common term is used, such as “data protection”, “data protection provisions”, “data protection information”, “data protection notice”<br>• In the case of complex, technical or unexpected processing operations, in addition to providing the information required under Art. 13 and 14 GDPR, a separate and clearly formulated description of the main consequences of the processing is provided<br>• The controller makes a documented assessment of whether there are any particular risks for the data subjects affected by the processing that should be brought to the attention of the data subjects. If this is the case, the data subjects are informed of these risks<br>• Use of multi-level data protection information/notice that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice<br>• The information is provided in as simple a manner as possible, avoiding complex sentence and linguistic structures<br>• Abstract and ambiguous terms or room for interpretation are avoided. |

| | |
|---|---|
| | • Modal verbs and words such as “can”, “could”, “some”, ‘often’ and “possible” are avoided<br>• Paragraphs and sentences are well-structured and hierarchical relationships are shown with bullet points and indents<br>• The information is written in the active rather than the passive voice and excessive nouns are avoided<br>• The information does not contain a disproportionate amount of legal, technical or specialized wording or terminology<br>• If the target audience of the data subject is children, the choice of words, tone and style of language is adapted to the child target group so that the child recipient of the information also recognizes that the message/information is addressed to them<br>• Information is provided in the national language of the respective target group, i.e. in German<br>• Information regarding data processing is provided in writing or by other means, including, where appropriate, by electronic means<br>• The information pursuant to Art. 13 and 14 GDPR may also be provided in electronic form (e.g. also contextual “just-in-time pop-up notices”, 3D touch notices and data protection dashboards, videos and smartphone or IoT voice messages, if applicable, in addition to multi-level data protection information/notices)<br>• In the event that a website is operated: Use of multi-level data protection information/notices that allow data subjects to go directly to specific points instead of displaying the entire information on the screen in the form of a single notice. Furthermore, when using multi-level data protection information/notices, the following must be ensured:<br>▪ The information pursuant to Art. 13 and 14 GDPR is also made easily accessible in a single place or in a single document (digital or paper format<br>▪ The design and organization of the first level of the multi-level data protection information/notice must provide the data subject with an overall view of the information available to them regarding the processing of their personal data and indicate where/how they can find the individual information at the respective levels of the data protection information/notice<br>▪ The information contained at the different levels of a multi-level notice is consistent and does not differ in a contradictory manner from level to level<br>▪ The first level of multi-level data protection information/notices contains information on the purposes of processing, the identity of the controller and the data subject: processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that will have the most significant impact on the data subject and the processing operations that the data subject may not expec<br>▪ The above information will be brought to the attention of the data subject directly at the time the personal data is collected, e.g. by displaying it on the screen while the |

| | |
|---|---|
| | data subject is filling out an online for<br>▪ With regard to the use of the multi-level approach in a non-digital environment: At the first level, at least the following information is communicated to the data subjects: Processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that has the most impact on the data subject and the processing operations that the data subject may not expect. It must be specified and documented how the further information required under Art. 13 and 14 GDPR is to be communicated<br>• Information on exercising rights regarding the processing of personal data (Articles 15–22 GDPR) is provided to the data subject.<br>• Processes for ensuring the right of access are established, see **DP06.11**.<br>• Data subjects affected by a breach of personal data protection will be informed, see **DP09.02**.<br>• Provision of information free of charge<br>▪ the controller does not charge a fee for the provision of information in accordance with Art. 13 and 14 GDPR or for notifications and measures taken in accordance with Art. 15 to 22 and Art. 34 GDPR<br>▪ The provision of information is not dependent on a financial transaction by the data subject<br>▪ Only in the case of manifestly unfounded or excessive requests from a data subject, particularly where they are repetitive, may the controller either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or b) refuse to act on the request. In such cases, the controller must provide evidence of the manifestly unfounded or excessive nature of the request.<br>• The following deadlines are observed with regard to the time at which information is provided:<br>a) In the case PD is collected from the data subject themselves:<br>• The information must be provided at the time the PD is collected, cf. Art. 13 para. 1 GDPR<br>b) In the case PD is not collected from the data subject directly<br>○ Information are communicated to the data subject within a reasonable period after obtaining the personal data “taking into account the specific circumstances of the processing of the personal data”, at the latest within one month (= maximum period) (Art. 14 para. 3 lit. a GDPR). With regard to the deadline, the following restrictions must be observed and, accordingly, earlier provision of the information must be ensure<br>○ If the personal data is used to communicate with the data subject: The information must be provided at the latest at the time of the first communication with the data subject (even if the latest deadline has not yet expired) (Art. 14 para. 3 lit. b GDPR |

- If disclosure of the personal data to another recipient is intended: The information must be provided at the latest at the time of this disclosure (even if the latest deadline has not yet expired) (Art. 14 para. 3 lit. c GDPR)

When deciding when to provide the information in accordance with Art. 14 GDPR, the legitimate expectations of the data subjects (what is the data subject's interest in being informed, i.e. how urgently is the information needed to exercise their rights), the potential impact of the processing on the latter and their ability to exercise their rights in relation to this processing must always be taken into account. The reasons for the decision as to why the information was provided at the specific time chosen must be documented by the controller. In accordance with the principle of good faith, the information must be provided as early as possible before the specified deadlines expire. The information obligation pursuant to Art. 14 para. 1 - 4 GDPR does not apply in the following cases, see Art. 14 para. 5 GDPR:

- The data subject already has the information. The controller must prove which information the data subject already has, how and when he received it, and that this information has not been subject to any significant changes in the meantime. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors.
- The provision of information proves to be legally or factually impossible or requires a disproportionate effort. The impossibility of providing information applies in particular to cases in which the controller does not know the data subject and therefore cannot inform the person. The controller must explain the factors that prevent it from providing the data subject with the information in question. When assessing whether the effort is disproportionate, the controller must weigh up the effort involved in providing the information against the interests of the data subject and document the result.
- There is still no obligation to provide information if providing such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Ar. 89 para. 1 GDPR or in so far as the obligation referred to in Art. 14 para. 1 GDPR is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available.

  It must be ensured that technical and organizational measures are in place to ensure, in particular, that the principle of data minimization is respected. Pseudonymization may also be one of the appropriate measures, provided

| | |
|---|---|
| | that it is possible to achieve these purposes in this way.<br><br>If the information pursuant to Art. 13 and 14 GDPR is changed significantly or factually (in particular in the event of a change in the purpose of processing, the identity of the controller, a change in the way in which the data subjects can exercise their rights with regard to processing, an extension of the categories of recipients, future transfer to a third country), the data subjects must be informed of the changes in good time before they actually take effect (at least 14 days in advance). There is no obligation to inform in the case of non-material changes. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors. The controller must ensure that the changes are communicated in a way that ensures that the majority of recipients actually pay attention to them. With regard to changes to the information in accordance with Art. 13 and 14 GDPR, the controller has implemented and documented processes which, in particular, make provisions for:<br>○ Specifications regarding the review and recording of any adaptation requirements for data protection information in the event of changes to processing activities (definition of responsibilities, communication channels, involvement of the data protection officer, documentation of adaptation requirements, sensitization of employees<br>○ Definition of responsibilities for making, approving and publishing changes to the data protection information<br>○ Determining how the changes will be communicated<br>▪ It must be ensured that the majority of recipients take note of the notification of changes (e.g. by email, by traditional letter on paper, by pop-up on a website or in another way that effectively brings the changes to the attention of the data subject<br>▪ The notification of changes must be separate from other information<br>▪ The information is provided in concise, transparent, intelligible and easily accessible form, using clear and plain language, see **DP06.01**<br>▪ The data subject is informed of the possible effects of these changes.<br><br>The fulfilment of the transparency principle by the Controller results from the overall fulfilment of the individual requirements referenced above.<br>Regarding the transparency of Data processing the "Guidelines on transparency under Regulation 2016/679 adopted on 29 November 2017 last revised and adopted on 11 April 2018 of the Article 29 Working Party" must be taken into account when applying this criterion. |

[GDPR] Art. 5 para. 1 lit. a

| | |
|---|---|
| **DP02.02** | **Controller** |

| | |
|---|---|
| | The evaluation object is designed to ensure that processing is carried out in a **fair manner (principle of fairness).** The Controller processes PD in a way that is not unjustifiably detrimental to the Data subject, unlawfully discriminatory, unexpected or misleading.The Controller implements the following measures as part of the fulfillment of the principle of fairness.<br>• the data subject is informed about the existence of the processing and its purposes cf. **DP02.01**, **DP06.01, DP06.04, DP06.05**, so that they can determine in advance the extent and consequences of the processing.<br>The following deadlines are observed with regard to the timing of the provision of information:<br>a) PD is collected from the data subject themselves<br>• The information (data protection information) is transmitted prior to the collection of the personal data, cf. Art. 13 para. 1 GDPR<br>b) Personal data is not collected from the data subject<br>• With regard to the timing of the information to the data subject, the following deadlines must be observed in accordance with Art. 14 para. 3 GDPR:<br>○ The information (data protection information) is communicated to the data subject within a reasonable period of time after obtaining the personal data "taking into account the specific circumstances of the processing of the personal data", at the latest within one month (= maximum period) (Art. 14 para. 3 lit. a GDPR). With regard to the deadline, the following restrictions must be observed and earlier provision of the information must be ensured accordingly.<br>○ If the personal data is used to communicate with the data subject: The information must be provided at the latest at the time of the first communication with the data subject (even if the latest deadline has not yet expired) (Art. 14 para. 3 lit. b GDPR).<br>○ If disclosure of the personal data to another recipient is intended: The information must be provided at the latest at the time of this disclosure (even if the latest deadline has not yet expired) (Art. 14. para. 3 lit. c GDPR)<br>○ When deciding when to provide the information in accordance with Art. 14 GDPR, the legitimate expectations of the data subjects (what is the data subject's interest in receiving the information, i.e. how urgently is the information needed to exercise their rights), the potential impact of the processing on the data subjects and their ability to exercise their rights in relation to this processing must always be taken into account. The reasons for the decision as to why the information was provided at the specific time chosen must be documented by the controller. In accordance with the principle of good faith, the information must be provided as early as possible before the expiry of the deadlines<br>The information obligation pursuant to Art. 14 para. 1 - 4 GDPR does not apply in the following cases, cf. Art. 14 para. 5 GDPR: |

| | |
|---|---|
| | ○ The data subject already has the information. The controller must prove which information is already available, how and when it received it, and that this information has not been subject to any significant changes in the meantime. Non-material changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors<br>○ The provision of information proves to be legally or factually impossible or requires a disproportionate effort. The impossibility of providing information applies in particular to cases in which the controller does not know the data subject and is therefore unable to inform the person. The controller must explain the factors that prevent it from providing the data subject with the information in question. When assessing whether the effort is disproportionate, the controller must weigh up the effort involved in providing the information against the data subject's interest in receiving the information and document the result.<br>○ There is still no obligation to provide information if the processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. However, the prerequisite for this is that the conditions and guarantees set out in Art. 89 para. 1 GDPR are met. It must be ensured that technical and organizational measures are in place to ensure, in particular, that the principle of data minimization is respected. Pseudonymization may also be one of the appropriate measures, provided that it is possible to achieve these purposes in this way<br>• The Controller provides information regarding Data processing in an objective and neutral manner, avoiding any misleading or manipulative language or design, cf. requirements in **DP06.01**.<br>○ The information is provided in as simple a manner as possible, avoiding complex sentence and linguistic structures<br>○ Abstract and ambiguous terms or room for interpretation are avoided.<br>○ Modal verbs and words such as “can”, “could”, “some”, ‘often’ and “possible” are avoided<br>○ Paragraphs and sentences are well-structured and hierarchical relationships are shown with bullet points and indents<br>○ The information is written in the active rather than the passive voice and excessive nouns are avoided<br>○ The information does not contain a disproportionate amount of legal, technical or specialized wording or terminology<br>○ If the target audience of the data subject is children, the choice of words, tone and style of language is adapted to the child target group so that the child recipient of the |

| | |
|---|---|
| | information also recognizes that the message/information is addressed to them<br>○ The information relating to data processing must be separated from other information that does not relate to data protection, e.g. contractual provisions, terms of use.<br>○ Use of a commonly used term, such as “data protection”, “data protection provisions”, “data protection information”, “data protection notice”<br>○ Information is provided in the national language of the respective target group, i.e. in German<br>• the processing of PD is based on a legal basis, see **DP03.01**<br>• the relevant legal bases are specifically communicated to the data subjects<br>• the controller has implemented processes regarding changes to the information in accordance with Art. 13 and 14 GDPR, cf. **DP06.01**<br>• The Controller takes measures to achieve an appropriate balance between its business interests and the rights and expectations of the data subjects, in particular in the case of online services offered without payment, where users are often unaware of how and to what extent their personal data are processed (only if the controller bases its data processing on a legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR), cf. requirements in **DP03.07**<br>• The Controller has processes implemented that enable the data subject to communicate and exercise their rights in relation to the processed personal data:<br>○ right of access, cf. **DP06.02, DP06.07, DP06.08, DP06.09**<br>○ right to rectification, cf. **DP06.02, DP06.11**<br>○ right to erasure, cf. **DP06.02, DP06.11**<br>○ right to restriction of processing, cf. **DP06.02, DP06.11**, **DP06.13**<br>○ right to data portability, cf. **DP06.02, DP06.14**<br>○ right to object, cf. **DP06.02, DP06.15**, **DP06.16**<br>○ right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject, cf. **DP06.17**<br>• The Controller ensures that it does not bind data subjects to its service in an unfair manner[2] (so-called lock-in). In context of a provider change, the Controller must enable data subjects to transfer their personal data to another Controller without this being associated with any particular effort or loss of data, cf. the requirements in **DP06.14**.<br>• If relevant: the reasonable expectations of the data subjects are taken into account by the Controller as part of a documented consideration |

[2] Business actions that are directed at or reach consumers are unfair if they do not comply with entrepreneurial diligence and are capable of significantly influencing the economic behaviour of the consumer.

| | |
|---|---|
| | in accordance with Art. 6 para. 1 lit. f GDPR. With regard to reasonable expectations, the Controller must take the following into account in particular:<br>○ a) whether there is a relevant and appropriate relationship between the data subject and the controller, e.g. if the data subject is a customer of the controller or is employed by the controller (cf. Recital 47 sentences 1 and 2 GDPR). In particular, the following elements must be taken into account when assessing the relationship with the data subject:<br>○ the existence of a relationship with the data subject (e.g. a distinction must be made between customers and non-customers), including the date of termination of the relationship, if such a relationship existed<br>○ proximity of the relationship (e.g. cases where a data controller is part of a group of companies with a single brand, compared to a group of companies that only has economic links unknown to the average customer, as in the latter case the data subject is less likely to expect data to be shared between the companies in the group)<br>○ Location and context of data collection (e.g. the data subjects may expect video surveillance in a bank, but not in sanitary or sauna facilities)<br>○ Type and characteristics of the service (e.g. a regular customer and a mere prospect who has only subscribed to a newsletter have different reasonable expectations)<br>○ Applicable legal requirements in the particular context (e.g. confidentiality requirements applicable to the relationship in question)<br>○ b) whether the data subjects can reasonably foresee at the time of the collection of the PD and the circumstances of the processing that processing may take place for this purpose (Recital 47 sentence 3 GDPR), i.e. that the processing is not surprising or unlikely, cf. requirements in **DP03.07**.<br>○ The fulfillment of the information obligations set out in Art. 12, 13 and 14 GDPR is not sufficient to assume that the data subjects can reasonably expect a certain processing, but can influence the data subject's expectation to a certain extent.<br>○ The “average” data subject must be considered in the assessment, unless the processing is likely to affect different groups of data subjects with different characteristics. The following characteristics must be taken into account: |

| | |
|---|---|
| | ○ Age of the data subject (the legitimate expectations of minors may be different from those of adults)<br>○ The extent to which the data subject is a public figure<br>○ The (professional) position held by the data subject and the degree of understanding and knowledge of the envisaged processing they are likely to have in a given context (e.g. staff involved in a job interview would often expect some of their personal data to be shared with job applicants).<br>• Where relevant: In the event of a change of purpose / further processing, the reasonable expectations of the data subject must be taken into account in the compatibility check pursuant to Art. 6 para. 4 GDPR (Recital 50 sentence 6), cf. the requirements in **DP03.08**<br>• where relevant: If the processing of personal data is based on algorithms, the Controller informs the data subject of the fact that the algorithms are used to create analyses or forecasts about them. The Controller regularly checks whether the algorithms are functioning appropriately. For this purpose, appropriate responsibilities, review intervals and the review methodology must be defined by the Controller. If errors are found, they must be rectified.<br>• In the event that automated decisions are made in individual cases, including profiling, the Controller provides for qualified human intervention to detect errors that may be caused by machines, cf. **DP06.17**.<br>The fulfilment of the principle of processing in a fair manner by the Controller results from the overall fulfilment of the individual requirements referenced above. |

[GDPR] Art. 5 para. 1 lit. a

| | |
|---|---|
| **DP02.03** | **Controller**<br>The evaluation object is designed in such a way that data **processing** is **based on a legal basis** (principle of lawfulness). In this context, the Controller must establish a correct legal basis for the processing of personal data.<br>1. The Controller must use the correct legal basis for data processing. The following legal bases must be taken into account:<br>a) The data subject has given their consent (Art. 6 para. 1 lit. a GDPR). Consent must be given voluntarily for the specific case, in an informed and unambiguous manner. Particular attention should be paid to the question of whether children and adolescents are in a position to express their informed consent, cf. the requirements in **DP03.02, DP04** and **DP04.09** (Consent of a child in relation to information society services)<br>b) the processing is carried out for the performance of a contract or the implementation of a pre-contractual measure (Art. 6 para. 1 lit. b GDPR), cf. the requirements in **DP03.03** |

| | |
|---|---|
| | c) the processing is necessary for compliance with a legal obligation to which the Controller is subject, see the requirements in **DP03.04**<br>d) the processing is carried out in order to protect the vital interests of the data subject or another natural person, cf. the requirements in **DP03.05**<br>e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (Art. 6 para. 1 lit. e GDPR), cf. the requirements in **DP03.06**<br>f) the processing is carried out to safeguard the legitimate interests of the Controller or a Third Party (Art. 6 para. 1 lit. f GDPR), cf. the requirements in **DP03.07**<br>g) if applicable: the requirements for further processing for a different purpose are met (Art. 6 para. 4 GDPR), cf. the requirements in **DP03.08**<br>2. If the requirements for the processing of special categories of personal data pursuant to Art. 9 GDPR are met, the Controller must meet the requirements in **DP05**<br>3. The Controller have to document the legal bases and the reason why the legal bases are relevant for the specific processing, cf. requirements in **DP03.01**<br>4. The controller informs data subjects about the relevant legal basis. , cf. requirements in **DP06.01**<br>5. The Controller differentiates between individual processing activities when selecting the correct legal bases, cf. requirements in **DP03.01**<br>6. The Controller ensures that the legal basis is clearly related to the purpose of the processing and that the processing is necessary and not subject to conditions, cf. requirements in **DP02.06**<br>7. The Controller determines the legal basis before the start of processing, cf. requirements in **DP03.01**<br>8. The Controller terminates processing as soon as the legal basis no longer applies and deletes the PD, cf. the requirements in **DP02.08**<br>9. The Controller ensures that the data subject can exercise control over the personal data as autonomously as possible within the framework of the legal basis.<br>10. If consent is the legal basis for processing, the controller must ensure that the data subject can withdraw their consent. Withdrawing consent should be as easy as giving it, cf. **DP04.06**.<br>11. if legitimate interests are the legal basis, the Controller must carry out a balancing of interests, taking into account in particular the imbalance of power, especially when children up to the age of 18 and other vulnerable groups are affected. Measures and safeguards are implemented to reduce the negative impact on the data subjects.<br>The fulfilment of the principle of lawfulness by the Controller results from the overall fulfilment of the individual requirements referenced above. |

[GDPR] Art. 5 para. 1 lit. b

| | |
|---|---|
| DP02.04 | **Controller**<br>The controller ensures that the purposes for which the PBD are processed are specified, explicit, and legitimate **(purpose limitation).**<br>The purpose of the processing is determined before the personal data is processed. The Controller documents the purpose of data processing. The Controller may only change the purpose of data processing in compliance with the derogations of article 6 sec. 4 GDPR (cf. DP03.08).<br>The controller has documented processes for selecting and implementing technical and organisational measures to ensure that personal data is processed for the intended purpose. The processes regulate in particular:<br>1. The Controller determines the purposes prior to data processing and assesses the purposes for which the data processing is to take place. The Controller determines responsibilities for carrying out an internal assessment of the purposes and records the procedure for this internal assessment. The personal data required for processing must then be determined based on the defined purpose.<br>2. The Controller documents the purposes in such a way that third parties are able to understand them. The Controller considers the following:<br>▪ The purpose must be specific; general statements such as 'for marketing purposes', 'improving the user experience', 'IT security purposes', 'future research' are not specific without further details. How detailed a purpose must be depends on the particular context in which the data is collected and on the personal data concerned.<br>▪ Abstract and ambiguous terms or terms with room for interpretation must be avoided.<br>▪ The description of purpose must not contain a disproportionate amount of legal, technical or specialised wording or terminology.<br>3. The Controller clearly defines the purposes (specificity)<br>4. The Controller checks and ensures that the processing is legally permissible for the specified purposes (legitimacy), cf. requirements in DP02.03.<br>5. The Controller implements technical and organisational measures to ensure that data records are not linked, i.e. that data records are not merged and that further processing for new purposes incompatible with the original purpose is prohibited.<br>6. The Controller implements organisational measures that restrict the reuse of personal data, e.g. contractual obligation of the Processors appointed, training of employees exist.<br>7. The Controller determines which personal data are necessary for the processing based on the purpose. The Controller reviews regularly whether the processing is necessary for the purposes for which the data was collected. In this context he implements appropriate processes (responsibilities, review intervals, review methodology).<br>8. The Controller implements processes to ensure that PD collected for one or more purposes is not further processed in a manner incompatible with those purposes. Any new purpose must be compatible with the original purpose for which the data was collected and must be taken into account when making changes to the design, see the requirements in DP03.08. |

| | |
|---|---|
| | 9. The controller uses technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The Controller also have organisational measures in place, such as policies and contractual obligations, which limit reuse of personal data.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 5 para. 1 lit. b

| | |
|---|---|
| **DP02.05** | **Controller**<br>Further processing of PD for archiving purposes in **the public interest, scientific or historical research purposes or statistical purposes** shall, in accordance with Art. 890 para. 1 GDPR, not be considered to be incompatible with the initial purposes (Art. 5 para. 1 lit. b sentence 2 GDPR, fiction of identity of purpose)<br>1. The controller must carry out an initial verification to determine whether the intended archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes can be achieved with anonymized data. The result of the verification must be documented. Responsibilities for the verification must be defined.<br>2. The controller must document the purposes of further processing and demonstrate that it is carried out for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes in accordance with Art. 89 para. 1 GDPR.<br>3. If the purposes cannot be achieved with anonymized data, the controller must demonstrate that technical and organizational measures (appropriate safeguards) are in place in accordance with Art. 89 para. GDPR, which in particular ensure compliance with the principle of data minimization, cf. **DS02.06**. In addition, measures to ensure other data protection principles, such as purpose limitation, confidentiality, and integrity of data, must also be taken into account, see **DS02.04**, **DS02.09**, **DS08.03**. The technical and organizational measures must be documented.<br>a) The Controller must ensure that the rights of data subjects are guaranteed, taking into account the exceptions set out in Article 89 para. 2, 3 and 4 GDPR. The Controller must document which regulations from EU law or German law pursuant to Art. 89 para. 2 and 3 are applied with regard to exceptions to the rights pursuant to Art. 15, 16, 18, 19, 20 GDPR.<br>b) Pursuant to Art. 89 para. 4 GDPR, the exception only applies to data processing for archiving, research or statistical purposes. If other purposes are also pursued, the exceptions to the rights of data subjects do not apply to these purposes.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 5 para. 1 lit. c

| | |
|---|---|
| **DP02.06** | **Controller**<br>The controller must ensure that the personal data processed are adequate, relevant and limited to what is necessary in relation to the purposes |

| | |
|---|---|
| | for which they are processed (**principle of data minimisation**).<br>The controller must first determine whether the processing of PD is necessary at all for its corresponding purposes. The Controller fulfills the principle of data minimisation in particular by the following aspects:<br>• Determining whether the purposes can be fulfilled by processing a smaller amount of personal data.<br>• Considering, whether less subdivided or aggregated personal data can be used. The Controller refrains from processing PD if it is possible for the relevant purpose.<br>• The Controller limit the amount of personal data collected to what is necessary for the purpose. The personal data must be relevant to the processing in question and the Controller must be able to demonstrate this relevance. The Controller must document why the data is necessary to achieve the purposes and must explain why the purposes or the processing without this PD could not be fulfilled (necessity test). The presentation of the necessity of the processing must take into account the entire life cycle of the data processing.<br>• The Controller must document why the purposes of the processing cannot reasonably be achieved to the same extent by other, more data-efficient means.<br>• If, within the evaluation object, there is a possibility that data subjects may make their PBD visible to other users or third parties, e.g., information from social media profiles, comments posted, the controller ensures that visibility is not the default setting and that the PBD is not made accessible to an indefinite number of natural persons without the data subject's intervention. Instead, data subjects can determine the scope of visibility of their PBD and the content they share themselves. The Controller provides technical options regarding the minimization of the processed personal data depending on the respective processing situation. For example, there are mandatory and optional fields for requesting personal data from the data subject.<br>• The Controller ensures that the number of persons who need access to personal data in order to carry out their tasks is as small as possible and that access is restricted accordingly. A role and authorization concept has been implemented for this purpose, which ensures that access is based on the need-to-know principle, cf. the requirements in **DP08.03**<br>• The Controller documents mechanisms, e.g. technical system configurations, that are implemented to ensure data minimization.<br>• Where possible, the Controller uses aggregated data.<br>• The Controller uses pseudonymization as soon as there is no longer any need for directly identifiable personal data, and identification keys must be stored separately. If pseudonymization techniques are used, the specific implementation is described.<br>• If the Controller does not need PD or no longer needs it for the purpose, it anonymizes or deletes it, cf. the requirements in **DP02.08**. The deletion must also take into account any backups.<br>• If anonymization techniques are used, the specific implementation is described.<br>• The controller does not create more copies than necessary when transferring data. |

| | |
|---|---|
| | • If the controller develops software that is used within the evaluation object, the principle of data minimization is already taken into account during the development of this software. The Controller sensitizes employees and compliance with the principle of data minimization and the development process is bindingly defined in the requirements for the development of software, e.g. privacy by design policy, coding policy, data protection policy.<br>• If data query fields, e.g., in forms, are used by the Controller within the evaluation object, only those PBD that are necessary for achieving the purposes are queried via mandatory fields. Free text fields are avoided. If free text fields are used, they are only mandatory fields in exceptional cases because the provision of further information is absolutely necessary to achieve the purpose. The controller must document why the use of mandatory free text fields is necessary to achieve the purposes and must explain why the purposes or the processing would not be achievable without this additional information (necessity test). The data subject must be given a transparent explanation of why the free text field exists and must be informed which information is desired and which is not, e.g., that the data subject should not enter any personal data.<br>• If goods or services are offered in e-commerce by the controller, data subjects must be offered guest access (online store without the creation of a permanent user account) or use of the IVS without registration. If guest access cannot be offered, the reasons for this must be documented.<br>• The Controller ensures, that access to external resources by the IPS (e.g. camera, calendar, address book, external devices) must be necessary to achieve the purpose. Technical measures must be taken to ensure that access only takes place to the extent necessary to achieve the purpose, i.e. only data records required for the processing purposes are accessed within the external resource. The data subject must be informed about access to external resources and consent to this access. Processes must be implemented that ensure a regular review of the need to access external resources and their data-saving implementation (definition of responsibilities, frequency of review, type of review).<br>• The Controller processes and stores data only in the most data-efficient format that allows the processing purposes to be fulfilled (e.g. recording age group instead of exact date of birth, recording occupational field instead of specific job title).<br>• The Controller implements technical and organizational measures that ensure the non-linking of data records, i.e. the merging of data records<br>Processes (Definition of responsibilities, type and manner of review) must be implemented to regularly review (at least annually or as circumstances require) whether the personal data being processed is still adequate, relevant and necessary, or whether the data must be deleted or anonymised. Responsibilities for the review must be defined.<br>The specification of the individual requirements can be found in the evaluation note. |

[GDPR] Art. 5 para. 1 lit. d

| | |
|---|---|
| DP02.07 | **Controller**<br>The Controller must keep PD correct and always up to date (**principle of accuracy**). In doing so, the Controller creates control and intervention options to determine the accuracy of PD and supports the correction and deletion of incorrect data.<br>• The Controller fulfills the principle of accuracy by taking the following measures. The Controller uses reliable sources regarding the accuracy of the processed personal data.<br>• The Controller must document, taking into account the type of PBD and its typical frequency of change, at what intervals and in what manner the data subject is requested to verify the accuracy of the personal data.The Controller informs data subjects about the processed PD and give effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed<br>• The Controller has established processes regarding correction, deletion and restriction requests, cf. the requirements in DP06.11<br>• The Controller regularly checks the correctness and accuracy of the data. Responsibilities, type and manner of the review and deadlines for the review must be defined for this purpose.<br>• The Controller minimizes the effects of a cumulative error in the processing chain. To this end, he should be able to trace the processing chain in all systems<br>• The structure of the data or database must be designed in such a way that individual data fields, data records or groups of data can be corrected, e.g. by the data subject.<br>• The Controller updates PD if necessary for the purpose<br>• The technical systems must be designed in such a way that rectification or erasure processes can be technically realised and that the data can be restricted for further processing in cases of doubt.<br>• The technical systems must be designed in such a way that corrections or deletions can be carried out without compromising the integrity of the data that remains unchanged.<br>• The Controller documents who is responsible for checking, ordering and carrying out corrections or deletions.<br>• An authorisation and role concept must ensure that unauthorised corrections or deletions can be prevented or subsequently detected.<br>• The Controller ensures that corrected or deleted data records are taken into account when restoring backups so that the possibility of incorrect data being used again for processing is effectively excluded<br>• The Controller ensures consistent further processing of the corrected data.<br>• The Controller documents all correction and deletion processes.<br>• The Controller ensures consistent further processing of the corrected data. |

| | |
|---|---|
| | • The Controller uses technical and organizational design features to reduce the incorrectness of data records, e.g. concisely formulated predefined answer options should be used instead of free text fields. |

[GDPR] Art. 5 para. 1 e, Art. 11, [DSK_17067] on Art. 5 para. 1 lit. e

| | |
|---|---|
| **DP02.08** | **Controller**<br>The Controller must ensure that the personal data is only stored for as long as it is necessary for the intended purposes (**principle of storage limitation**).**Identification of the data subject** when storing their personal data is only possible for as long as is necessary for the purposes of the processing.<br>Personal data must be stored in a form which permits identification of data subjects only for as long as is necessary for the purposes for which they are processed. The data must then be deleted (in the physical sense) or irreversibly anonymised. If anonymisation is carried out, it must be completely irreversible.<br>The Controller has a documented deletion concept, e.g. in accordance with DIN 66398-2016, which regulates the following :<br>• Scope of the deletion concept (e.g. which IT systems and databases)<br>• Definition of deletion periods<br>• Definition and concrete description of deletion mechanisms (documentation of the individual processes and implementation specifications)<br>  ○ When defining the minimum requirements for deletion procedures, the specifications of the BSI IT-Grundschutz-Compendium CON.6 Deletion and destruction must be met<br>• Definition of responsibilities and reporting channels with regard to the execution of deletions<br>• The Controller must be able to justify why the duration of storage is necessary for the purpose and in relation to the personal data processed and must be able to provide the justification and legal basis for the storage period.<br>• If a processor is used by the controller: Explanation o which deletion obligations are to be fulfilled by the processor<br>• Responsibilities with regard to monitoring the deletion processes<br>• Verification of the actual implementation and validity of the deletion<br>• Definition of how deletions are documented<br>• Inclusion of data deletion in backups and archives<br>• Regular evaluation (at least annually) of the selected deletion mechanisms to determine whether they still correspond to the state of the art<br>• The Controller implements automated deletion procedures where possible.<br>• The Controller determines which personal data and which storage duration are necessary for backups and log files.<br>It must be ensured that deletions can be carried out without compromising the integrity of the remaining data.<br>Opinion 5/2014 of the Article 29 Working Party on Anonymisation Techniques, WP 216, must be taken into account as a benchmark for assessing whether effective de facto anonymisation exists. |

| | |
|---|---|
| | According to this, it must not be possible for any party to anonymise personal data,<br>▪ to pick out a person from a database,<br>▪ to link data records relating to a person, e.g. to create a link between two data records of a data set (or between two independent data sets), or<br>▪ deriving information about a person from such a database by means of inference.<br>Due to technological progress, there is a risk that anonymised data may be de-anonymised, meaning that the validity of the anonymisation must be continuously checked. Corresponding processes must be implemented and documented. The processes must, in particular, specify: Responsibilities for verifying the validity of the anonymization procedures, Method of verification (e.g., re-identification attacks), scope of the verification (random or comprehensive) frequency of the verification (at least annually or as required), documentation of the verification, definition of procedures if de-anonymization is detected.<br><br>There are clear rules between the Processor and Controller, see Art. 28 para. 3 lit. g GDPR, DP07.09, on what must happen to the personal data after termination of the contract (deletion, return). There is a process in place for handing over the personal data to the Controller or deleting the personal data after termination of the contract (determination of responsibilities, manner of handing over the PD or deletion). This also takes into account all personal data held by any other Processors.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 5 para. 1 lit. f

| | |
|---|---|
| DP02.09 | **Controller**<br>Personal data are processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through appropriate technical and organisational measures, see the requirements in DP08. |

[GDPR] Art. 5 para. 2

| | |
|---|---|
| DP02.10 | **Controller**<br>The Controller must be able to demonstrate compliance with the aforementioned criterion as part of their accountability.<br>The measures for compliance with the requirements of criteria DP02.01 to DP02.09 are documented.<br>The responsibility structure within the established data protection management system and the individual process descriptions is documented, cf. the individual requirements in DP09. |

## DP03 Lawfulness of processing

[GDPR] Art. 6 para. 1

| | |
|---|---|
| DP03.01 | **Controller**<br>Processing shall be lawful only if and to the extent that at least one of the following applies:<br>1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes,<br>2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,<br>3. processing is necessary for compliance with a legal obligation to which the controller is subject,<br>4. processing is necessary in order to protect the vital interests of the data subject or of another natural person,<br>5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,<br>6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.<br>The Controller has implemented processes that ensure an upstream check of the existence of a legal basis.<br>These processes apply in particular to the following definitions:<br>• Definition of responsibilities for carrying out the review, including the involvement of certain departments<br>• Definition of how the lawfulness review is carried out: It should be evident from the lawfulness check that the controller checks all the conditions specified in Art. 6 para. 1 lit. a - f GDPR for relevance and reaches a conclusion. The process should show the regularity of the review of lawfulness and take the following aspects into account:<br>○ the applicable national data protection law<br>○ the necessity of the data processing with regard to whether the data is necessary to achieve the purpose and whether the purpose of the processing cannot reasonably be achieved by other means<br>○ any joint controllership pursuant to Art. 26 GDPR<br>○ processors involved pursuant to Art. 28 GDPR<br>○ data recipients involved.<br>○ Documentation of the legal basis<br>Processes must be implemented to ensure that data processing only takes place once the data processing agreement has been effectively concluded. This is regulated as a minimum:<br>• Documentation of how contracts are awarded (procurement channels/process) |

| | |
|---|---|
| | • Guidelines for the commissioning of service providers (e.g. purchasing policy)<br>• Specification of when data protection officers are to be involved<br>• Existence of sample data processing agreements according to Art. 28 GDPR<br>• Specification of responsibilities with regard to the review of whether a data processing agreement according to Art. 28 GDPR must be concluded<br>• Definition of responsibilities with regard to the review of data processing agreements<br>• Definition of responsibilities for the conclusion of the data processing agreement (signature regulation)<br>• Documentation of the conclusion of the data processing agreement<br>• Documentation of the data processing agreement in accordance with established document management<br>The specification of the individual requirements can be found in the evaluation notes. |

The following criteria describe the individual bases of lawfully processing and are applicable or obsolete depending on the basis of the processing. They may refer to other relevant criteria in this document.

[GDPR] Art. 6 para. 1 lit. a

| | |
|---|---|
| **DP03.02** | **Controller**<br>If the processing is based on consent (Art. 6 para. 1 lit. a GDPR), the lawfulness requirements pursuant to DP04 must be met.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 6 para. 1 lit. b in conjunction with Art. 5 para. 1 lit. c

| | |
|---|---|
| **DP03.03** | **Controller**<br>If the processing is **carried out** for the **performance of a contract** or **the implementation of a pre-contractual measure** (Art. 6 para. 1 lit. b GDPR), the following requirements must be met.<br>1. The contract with the data subject, to which the processing relates, must<br>a) actually exist effectively or<br>b) it must be a pre-contractual relationship at the request of the data subject.<br>2. Purposes of the processing in the context of a contractual relationship are clearly defined and communicated to the data subject.<br>3. Data processing must<br>a) be objectively necessary for the performance of a contract with a data subject, or<br>b) objectively necessary for the performance of pre-contractual measures taken at the request of the data subject. |

| | |
|---|---|
| | Only those personal data are processed that are absolutely necessary for the performance of a contract or for the implementation of pre-contractual measures (see **DP02.06**, Art. 5 para. 1 lit. c GDPR).<br>Furthermore, all processing operations are necessary for the performance of a contract or for the implementation of pre-contractual measures.<br>It must be demonstrated to what extent the main purpose of the contract with the data subject cannot be fulfilled if the specific processing of the personal data in question does not take place.<br>4. The structures and processes that lead to the conclusion of a contract or a pre-contractual relationship are documented.<br>5. Insofar as Art. 6 para. 1 lit. b GDPR forms the basis for some or all processing operations, processes are in place with regard to any contract cancellations with regard to the resulting consequences for data processing. Regulations must be made with regard to the cessation of processing, deletion of data (cf. Art. 17 para. 1 lit. a GDPR) and any existing exceptions to the deletion obligation, e.g. fulfillment of a legal obligation pursuant to Art. 17 para. 3 lit. e GDPR. The requirements pursuant to **DP02.08** must be taken into account accordingly<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 6 para. 1 lit. c in conjunction with Art. 5 para. 1 lit. c, Art. 6 para. 2, 3

| | |
|---|---|
| **DP03.04** | **Controller**<br>If the processing is carried out to fulfil a legal obligation to which the Controller is subject (Art. 6 para. 1 lit. c GDPR), the following legality requirements must be met.<br>1. The existence of a legal obligation on the Controller and the obligation must relate directly to data processing.<br>2. The obligation is related to the data subject.<br>3. The legal obligation must arise from European Union law or German law to which the Controller is subject. The legal obligation must fulfil the requirements of Art. 6 para. 2 and 3 GDPR or any existing special regulations (e.g. legal obligations in collective agreements).<br>4. It must be documented which legal basis from European Union law or German law in conjunction with Art. 6 para. 1 lit. c GDPR is used.<br>5. Processing must be necessary for compliance with a legal obligation (cf. **DP02.06**, Art. 5 para. 1 lit. c GDPR).<br>The specification of the individual requirements can be found in the evaluation note. |

[GDPR] Art. 6 para. 1 lit. d in conjunction with Art. 5 para. 1 lit. c

| | |
|---|---|
| **DP03.05** | **Controller**<br>If the processing is carried out in order to protect the vital interests of the data subject or another natural person (Art. 6 para. 1 lit. d GDPR), the following lawfulness requirements must be met.<br>1. The existence of vital interests of the data subject or another natural person.<br>2. It must be documented whose and which vital interests are affected. |

| | |
|---|---|
| | 3. The processing must be necessary for the protection of vital interests (cf. (cf. **DP02.06**, Art. 5 para. 1 lit. c GDPR).<br>4. No other legal basis is relevant.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 6 para. 1 lit. e in conjunction with Art. 5 para. 1 lit. c, Art. 6 para. 2, 3

| | |
|---|---|
| **DP03.06** | **Controller**<br>If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (Art. 6 para. 1 lit. e GDPR), the following conditions of lawfulness must be met.<br>1. The Controller was a) entrusted with the performance of a task carried out in the public interest or b) entrusted with tasks carried out in the exercise of official authority. The conditions for the fulfilment of the task, its scope and the circumstances that lead to the legal basis ceasing to apply must be documented.<br>2. The legal basis for data processing must be derived from European Union law or German law to which the Controller is subject. The legal basis must fulfil the requirements of Art. 6 para. 2 and 3 GDPR and any existing special regulations (depending on the context of application).<br>3. It must be documented which legal basis from European Union law or German law in conjunction with Art. 6 para. 1 lit. e GDPR is used.<br>4. The processing must be necessary for the performance of the task (cf. **DP02.06**, Art. 5 para. 1 lit. c GDPR).<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 6 para. 1 lit. f

| | |
|---|---|
| **DP03.07** | **Controller**<br>If the processing is carried out to protect the legitimate interests of the Controller or a third party (Art. 6 para. 1 lit. f GDPR), the following legal requirements must be met.<br>1. The processing must be in the legitimate interest of a) the Controller or b) a third party.<br>2. These are not processing operations carried out by a public authority in fulfilment of its tasks.<br>3. Data processing must be necessary for the intended purpose.<br>4. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.<br>5. The reasonable expectations of the data subjects must be taken into account With regard to reasonable expectations, the following must be taken into account:<br>a) whether there is a significant and appropriate relationship between the data subject and the controller, e.g. if the data subject is a customer of the controller or is in the controller's service (see Recital |

47, sentences 1 and 2 of the GDPR). In particular, the following elements must be taken into account when assessing the relationship with the data subject:

- Existence of a relationship with the data subject (e.g., a distinction must be made between customers and non-customers), including the date of termination of the relationship, if such a relationship existed
- Proximity of the relationship (e.g., cases where a controller is part of a group of companies with a single brand, as opposed to a group of companies that only has economic links that are unknown to the average customer, since in the latter case the data subject is less likely to expect data to be shared between companies within the group)
- Location and context of data collection (e.g., data subjects may expect video surveillance in a bank but not in sanitary or sauna facilities)
- Nature and characteristics of the service (e.g., a regular customer and a mere prospect who has only subscribed to a newsletter have different reasonable expectations)
- Applicable legal requirements in the specific context (e.g., confidentiality requirements applicable to the relationship in question)

b) whether, at the time of collection of the personal data and in the circumstances of the processing, the data subjects can reasonably foresee that processing for that purpose may take place (Recital 47, sentence 3 GDPR), i.e., that the processing is not surprising or unlikely.

- Simply fulfilling the information obligations set out in Articles 12, 13, and 14 GDPR is not sufficient to assume that data subjects can reasonably expect a particular processing operation.
- When weighing up the interests, the “average” data subject must be considered, unless the processing is likely to affect different groups of data subjects with different characteristics. The following characteristics must be taken into account:
  - Age of the data subject (the legitimate expectations of minors may differ from those of adults)
  - Extent to which the data subject is a public figure
  - The (professional) position held by the data subject and the degree of understanding and knowledge of the intended processing that they are likely to have in a specific context (e.g., personnel involved in a job interview would often expect some of their personal data to be shared with the applicants).

6. The interests must be balanced by taking additional protective measures into account.
7. The balancing of interests must be documented in a transparent and addressee-orientated manner.
8. the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.

The specification of the individual requirements can be found in the evaluation notes.

[GDPR] Art. 6 para. 4

| | |
|---|---|
| DP03.08 | **Controller**<br>If the Controller intends to process PD for a purpose other than that for which the PD was collected, the Controller must document all purpose changes with reasons. It must be clear what the original purpose was and what purpose is now being pursued with the processing.<br>The Controller has documented processes in place to check the lawfulness of a change of purpose and with regard to further measures (e.g. obtaining further consent). In this context, responsibilities for reviewing the legality of a change of purpose, the manner of the review (documentation of the review procedure, taking into account the review steps listed below), sensitization of employees regarding the handling of any changes of purpose, involvement of the data protection officer, as well as the documentation of the implementation of the review are defined.<br>If a purpose change is intended, the Controller must check whether the processing for another purpose is lawful. In this context, the Controller has a documented review process (See above for process requirements) which ensures that the following process steps are carried out:<br>a) Review, if a corresponding consent of the data subject has been obtained, cf. requirements in DP04<br>b) Review, if a legal provision of the Union or a German legal provision is applicable<br>• The change of purpose may have its legal basis in a legal provision of the European Union or the member states if this constitutes a necessary and proportionate measure in a democratic society to protect the common interests of Art. 23 para. 1 GDPR. If it is a German regulation, Germany must also have a regulatory power for the initial processing (i.e. in particular on the basis of Art. 6 para. 1 lit. c and lit. e in conjunction with para. 2 and 3 GDPR), cf. requirements in DP03.05 and DP03.06.<br>If the processing for a purpose other than that for which the data was collected is not based on consent or a legal provision of the Union or a German legal provision, the Controller conducts a documented assessment in accordance with Art. 6 sec. 4 GDPR **(compatibility test)** and considers the following test steps:<br>**1. Check purpose limitation**<br>Link between the purposes for which the personal data were collected and the purposes of the intended further processing<br>• Recording the original purpose of the data collection<br>• Determining whether the new purposes of the processing are compatible with the original purpose<br>Purpose limitation can be assumed in particular if the original purpose has already implied the new purpose of further processing as the logical next step.<br>**2. Check the context of data processing** |

| | |
|---|---|
| | The context in which the personal data was collected, in particular with regard to the relationship (e.g. buyer and seller, employer and employee) between the data subjects and the Controller<br>• Check whether the initial information comprehensively refers to possible scenarios of further use.<br>• Examination of whether the change of purpose can be regarded as foreseeable from the perspective of the data subject. The reasonable expectations of the data subject based on their relationship with the controller with regard to the further use of this data must be taken into account (see recital 50 sentence 6 GDPR). The following must be taken into account:<br>○ Whether the data subject is in a closer relationship with the controller (e.g. customer relationship, employment relationship), including the date of termination of the relationship, if any<br>○ Proximity of the relationship (e.g. cases where a data controller is part of a group of companies with a single brand compared to a group of companies that only has economic links that are unknown to the average customer, as in the latter case the data subject is less likely to expect data to be shared between the companies in the group)<br>○ Link between the initial processing purpose at the time of collection and the purposes of the envisaged further processing (is the processing already implicit in the initial purpose and can it be seen as a logical next step)<br>○ Is the further processing in line with common practice in the context, so that the processing is not unexpected and unforeseeable (context of the further processing)<br>○ Is the further processing based on a legal provision<br>○ Transparency of the further processing (including the nature and content of the information initially or subsequently provided to the data subject)<br>However, mere compliance with the information obligations laid down in Art. 12, 13 and 14 GDPR is not sufficient to assume that the data subjects can reasonably expect a certain processing, but may influence the data subject's expectation to a certain extent.<br>○ Applicable legal requirements in the respective context (e.g. confidentiality requirements that apply to the relationship in question)<br>**3. Consideration of the type of PD**<br>If particularly sensitive data, such as special categories of personal data pursuant to Art. 9 GDPR are to be processed, there is an increased need for justification as part of the compatibility check pursuant to Art. 6 para. 4 GDPR (possibly in conjunction with Art. 5 para. 1 lit. b GDPR).<br>Other sensitive data, such as personal data of children and the elderly, must also be taken into account, especially in the context of the compatibility test.<br>**4. Consequences for the data subject** |

| | |
|---|---|
| | A change of purpose may increase the risk to the rights and freedoms of the data subjects.<br>• Review the requirement to carry out a data protection impact assessment pursuant to Art. 35 GDPR<br>• Comparison of positive and negative consequences for the data subject (e.g. economic and social advantages and disadvantages)<br>• Consideration of whether further processing by the Controller who has already collected the data or a third party gains knowledge of the personal data through further processing. The existence of an increased risk when transferring personal data to third parties who process data for a different purpose, e.g. due to uncontrollable parallel storage for which protective measures such as access restrictions and blocking could be lost<br>• Checking whether the systems and processes continue to guarantee the exercise of data subject rights in accordance with chapter 3 GDPR after the change of purpose<br>• Updating the information to the data subject within the meaning of Art. 13 or 14 GDPR (e.g. data protection information)<br>• Review of the effects on existing data processing agreements and, if necessary, adjustment of the relevant data processing agreements<br>The more difficult it is for the data subject to understand the further processing in detail and to assess the consequences, the more likely it is that purpose compatibility must be rejected.<br>**5. Existence of Appropriate safeguards**<br>By implementing suitable technical and organisational measures, it is possible to compensate for the risks associated with a change of purpose. The following exemplary measures can be used as suitable safeguards:<br>▪ Check whether the same purpose can be achieved with further processing through encryption or pseudonymisation<br>▪ Anonymisation of personal data<br>▪ Aggregation of personal data<br>▪ Implementation of privacy enhancing technologies<br>Privacy-friendly default settings |

## DP04 Consent

[DSGVO] Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 Abs. 2

| | |
|---|---|
| DP04.01 | **A) Controller**<br>If the controller processes personal data on the basis of consent, the data subject must have consented to the processing of their personal data for one or more specific purposes.<br>Consent is given for a specific purpose:<br>• the consent of the data subject is given for "one or more specific" purposes and the data subject has a choice in relation to each of these purposes<br>• The consent covers all processing operations carried out for the same purpose or purposes<br>• If the processing serves multiple purposes, the data subject may give separate consent for different processing activities.<br>• With each request for separate consent, the controller provides specific information about the data that will be processed for each purpose, so that the data subjects are aware of the implications of the different choices.<br>The following conditions for the validity of consent are fulfilled by the controller.<br>Specific verification is carried out in the following criteria.<br>1. Freely given declaration of consent, see requirements in DP04.02<br>2. Declaration of consent given for a specific purpose, DP04.03<br>3. informed declaration of consent, DP04.03<br>4. unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, DP04.04<br><br>**B) Processor**<br>As part of its obligation to follow instructions, the processor supports the Controller in obtaining consent, if the Controller has expressly instructed the processor (cf. the requirements in DP07.04, DP07.10) that the processor is responsible for obtaining consent from the data subjects on behalf of the controller. If there is no corresponding instruction, this criterion is not applicable. The content of the consent declaration is the responsibility of the controller and must be implemented by the processor. The Processor has to inform the controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions. The responsibilities and communication channels for this must be documented. |

[GDPR] Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 para. 4

| | |
|---|---|
| DP04.02 | **Controller**<br>The Consent is given by the data subject freely. With regard to the assessment of the freely given consent, the following aspects must be considered in particular:<br>• The data subject has a genuine and free choice and is able to refuse or withdraw consent refuse or withdraw consent without suffering any disadvantages (i.e. without the risk of deception, intimidation, coercion or other significant adverse consequences (e.g. additional costs)). The Controller must provide evidence of this.<br>• Consent is not freely given if the data subject is in a situation of dependency on the controller due to the nature of their relationship or due to special circumstances, cf. the comments in the test on imbalance of power.<br>• Access to services and functions may not be made dependent on the consent of a data subject to the storage of information in their device or access to information already stored therein (so-called cookie banners or cookie walls).<br>• The process/procedure for obtaining consent must allow data subjects to give separate consent for different processing operations and processing purposes of PD (i.e. only for some processing operations or purposes and not for others).<br>• The Controller must be able to prove that the data subject has voluntarily consented to the processing of the personal data. The Controller must document the reasons why consent is freely given.<br>• The Controller must demonstrate that the withdrawal of consent will not result in costs for the data subject and will not be disadvantageous for those who withdraw consent.<br>• It is not freely given if the withdrawal of consent is associated with additional effort for the data subject, e.g. clicks or attention, signing an additional form to withdraw consent, if the withdrawal of cookies is only possible at the second cookie banner level, if an extra button must be clicked to withdraw consent.<br>• It is not freely given if a cookie banner or other graphic element for requesting consent obscures access to the IPS as a whole or parts of the content and the cookie banner cannot simply be closed without a decision.<br>• It is not freely given if an opt-out must be made by the data subject.<br>• It is not freely given if all cookies are already preselected and are activated by clicking on the ‘Allow cookies’ button.<br>• It is not freely given if the data subject is forced to give consent by means of manual colour combinations or complicated selection processes (nudging or dark patterns).<br>• It is not freely given if information is formulated in a misleading way, if deliberately trivialising language is used or if the data subject is overloaded with information.<br>• Consent is not freely given if the possibility of withdrawing consent is not clearly recognisable to the data subject because, for example, it is placed outside the consent banner or is difficult to read.<br>• When assessing whether consent is freely given, it must be taken into account whether the fulfilment of a contract is made dependent on |

| | |
|---|---|
| | consent being given to data processing that is not necessary for the fulfilment of the contract. If this is the case, this regularly means that the consent cannot be regarded as freely given.<br>• Consent is given for a specific purpose:<br>  ○ the consent of the data subject is given for “one or more specific” purposes and the data subject has a choice in relation to each of these purposes<br>  ○ The consent covers all processing operations carried out for the same purpose or purposes<br>  ○ If the processing serves multiple purposes, the data subject may give separate consent for different processing activities.<br>  ○ With each request for separate consent, the controller provides specific information about the data that will be processed for each purpose, so that the data subjects are aware of the implications of the different choices. |

[GDPR] Art. 4 Nr. 11, Art. 7 para. 2

| | |
|---|---|
| **DP04.03** | **A) Controller**<br>The **consent is given informed** by the data subject. It contains at least the following information:<br>1. the identity of the Controller,<br>2. the categories of data processed,<br>3. the processing phases of the respective PD,<br>4. planned transfers and recipients of the transfer,<br>5. the purpose of data processing,<br>6. it is given voluntarily,<br>7. revocability and the consequences of withdrawal<br>8. if relevant: information on possible risks of data transfers into countries without an adequacy decision and without appropriate safeguards in accordance with Art. 46 GDPR<br>9.if relevant: on the use of the data for automated decision-making<br><br>The information is provided in particular in the form of written or verbal explanations or audio or video messages<br>Depending on the circumstances and context of each case, more information may be required with regard to informed consent, see the requirements for Art. 13 GDPR in **DP06.04**.<br><br>Information is provided as follows:<br>1. intelligible and easily accessible form<br>• The information is not hidden, i.e., the data subject must not be forced to search for the information themselves.<br>• It must be easy for data subjects to identify who the controller is.<br>• The declaration of consent is identified as such. Misleading headings that mislead data subjects about the actual content are not used. |

| | |
|---|---|
| | • Manipulative color combinations or complicated selection processes (nudging or dark patterns) that pressure data subjects into giving their consent are not used.<br>• The content is guaranteed to be accessible at all times.<br>• The information that is relevant for making an informed decision is not hidden in general terms and conditions.<br>• If consent is to be given electronically, the request must be made in a clear and concise manner. Multi-layered and separate information is possible in order to fulfill the dual obligation of being precise and complete on the one hand and understandable on the other.<br>• If the request for consent is made electronically, the request for consent is made in a clear and concise form and without unnecessary interruption of the service for which consent is given.<br>2. in clear and plain language, cf. **DP06.01**<br>• The wording is tailored to the target group. If the target group includes minors, the information is provided in clear and simple language that a child can understand. It must be ensured that the wording, tone, and style of language are appropriate for the child audience.<br>• The declaration of consent is formulated in the national language of the country in which the controller is seeking consent. The declaration of consent must therefore be written in German.<br>• The information is provided in the simplest possible manner, avoiding complex sentence and linguistic structures.<br>• Abstract and ambiguous terms or room for interpretation are avoided.<br>• Modal verbs and words such as “can,” “could,” “some,” “often,” and “possible”are avoided.<br>• Paragraphs and sentences are well structured and hierarchical relationships are represented using bullet points and indents.<br>• The information is written in the active voice and not in the passive voice, and excessive nominalization is avoided.<br>• The information does not contain an excessive amount of legal, technical, or specialized wording or terminology.<br>• It is clear who is the controller.<br>• The purpose of the data processing for which the data processing is to be carried out is clearly explained.<br>• The declaration of consent is named as such.<br>3. clearly separated from other matters<br>• If the consent relates to other matters, the request for consent is made in an intelligible and easily accessible form, using clear and plain language, so that it is clearly distinguishable from other matters<br>• If consent is requested in the context of a contract (in writing), the request for consent is clearly distinguished from other matters.<br>• If the written contract contains many aspects that are not related to |

| | |
|---|---|
| | the question of consent to the use of PD, the question of consent is dealt with either in a separate document or in a manner that is clearly distinguishable.<br>• The information relevant to the decision in informed references is easily recognizable to the data subject and not hidden (e.g., in general terms and conditions), in particular by means of a highlighted graphic design, such as a border, colored or gray background for the consent declaration, the use of special fonts and font designs (bold; italics) or other design features that clearly highlight the declaration of consent and do not hide it in general terms and conditions.<br>• If the request for consent is made electronically, it is provided in a separate and clear form in accordance with Recital 32 GDPR and not merely as a paragraph in the terms and conditions.<br><br>**B) Processor**<br>As part of its obligation to follow instructions, the processor supports the Controller in obtaining consent, if the Controller has expressly instructed the processor (cf. the requirements in **DP07.04, DP07.10**) that the processor is responsible for obtaining consent from the data subjects on behalf of the controller. If there is no corresponding instruction, this criterion is not applicable. The content of the consent declaration is the responsibility of the controller and must be implemented by the processor. The Processor has to inform the controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions. The responsibilities and communication channels for this must be documented. |

[GDPR] Art. 4 Nr. 11

| | |
|---|---|
| **DP04.02** | **A) Controller**<br>Consent is given by means of a statement or by a clear affirmative action by the data subject.<br>• Consent is given in the form of a written declaration, which may also be given electronically, or a verbal declaration or any other declaration or conduct by which the data subject clearly indicates in the given context that he or she agrees to the intended processing of his or her personal data, e.g. by ticking a box, selecting technical settings for information society services<br>• Silence, pre-ticked boxes, opt-out mechanisms, mere information and continued use of the IPS, or inactivity do not constitute consent.<br>• Consent to the processing of PD is obtained separately from any process by which a contract or general terms and conditions are accepted.<br>• Consent is obtained before processing of PD begins.<br><br>**B) Processor**<br>As part of its obligation to follow instructions, the Processor supports the Controller in obtaining consent, if the Controller has expressly instructed |

| | |
|---|---|
| | the processor (cf. the requirements in **DP07.04, DP07.10**) that the processor is responsible for obtaining consent from the data subjects on behalf of the controller. If there is no corresponding instruction, this criterion is not applicable. The way in which the declaration of consent is made accessible and visible is determined by the Controller's instructions, which must be fulfilled accordingly by the Processor. The Processor has to inform the controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions. The responsibilities and communication channels for this must be documented. |

[GDPR] Art. 7 para. 1

| | |
|---|---|
| **DP04.03** | **A) Controller**<br>If processing is carried out on the basis of the data subject's consent, the Controller is able to demonstrate that the data subject has given consent to the processing operation.<br>In particular, the Controller can demonstrate:<br>• The content of the declaration of consent (Consent to which processing activities, which PD, for which purposes?)<br>• Proof that the data subject was provided with all necessary information prior to giving consent so that they could make their decision on the basis of comprehensive information<br>• Procedures for obtaining consent, including details of the information provided to the data subject<br>• Proof that all criteria for valid consent have been met (documentation of the individual processes relating to the granting of consent at the time it was given and documentation of the information provided to the data subject at that time)<br>When providing proof that valid consent has been obtained, only data that is necessary to prove the specific consent will be collected, see **DP02.06**.<br>The obligation to provide proof shall remain in force for as long as data processing activities continue. After the processing activity has been completed, the proof of consent will only be retained for as long as is necessary to fulfill a legal obligation or to assert, exercise, or defend legal claims in accordance with Article 17(3)(b) and (e). Appropriate deletion processes have been established for this purpose, which in particular specify:<br>• Retention period for proof of consent<br>• Responsibilities for deletion<br>• Procedure for implementing deletion<br>• Responsibilities for reviewing the implementation of deletions, including determining the type and frequency of reviews<br><br>**B) Processor**<br>As part of its obligation to follow instructions, the Processor supports the Controller in providing proof that the data subject has given consent, if the Controller has expressly instructed the processor (cf. the requirements in **DP07.04, DP07.10**) that the processor is responsible for obtaining consent from the data subjects on behalf of the controller and for the docu- |

| | |
|---|---|
| | mentation of the consent. If there is no corresponding instruction, this criterion is not applicable. |

[GDPR] Art. 7 para. 3

| | |
|---|---|
| DP04.04 | **A) Controller**<br>**Withdrawal of consent** is just as easy as giving consent. With regard to the withdrawal of consent, the following requirements must be fulfilled by the controller:<br>• When consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily.<br>• If consent is given directly when using the IPS, it must also be possible to withdraw consent in this way.<br>• If consent is t is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), the data subject must be<br>• able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Exclusive withdrawal options via other communication channels such as e-mail, fax or letter are not appropriate. An exclusive reference to a contact form is not appropriate.<br>• If consent is obtained via a banner or similar, it is inadmissible if a data protection information must first be viewed and then scrolled to the correct section in order to reach a withdrawal option.<br>• A placement of the withdrawal option in the data protection information is only permissible if links in the data protection information direct the data subject directly to the section on the possibility of withdrawal and no search processes are necessary (directly accessible withdrawal option).<br>• The data subject must be able to withdraw their consent without suffering any detriment, i.e. withdrawal must be possible free of charge and without lowering service levels. The Controller must document how the data subject can withdraw the consent.<br><br>**B) Processor**<br>As far as possible, the processor supports the controller as part of its obligation to follow instructions, to enable the withdrawal of consent as easily as the granting of consent.<br>As part of its obligation to follow instructions, the Processor supports the Controller to enable the withdrawal of consent as easily as the granting of consent, if the Controller has expressly instructed the processor (cf. the requirements in **DP07.04, DP07.10**) that the processor is responsible for obtaining consent from the data subjects on behalf of the controller and for the documentation of the consent. If there is no corresponding instruction, this criterion is not applicable. |

[GDPR] Art. 7 para. 3

| | |
|---|---|
| DP04.05 | **A) Controller**<br>Before consent is given, The Controller informs the data subject that the withdrawal of consent does not affect the lawfulness of the **processing carried out** on the basis of the consent **until the withdrawal.**<br><br>**B) Processor**<br>The Processor assists the Controller as part of its obligation to follow instructions in informing the data subject, before consent is given, that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. |

[GDPR] Art. 7 para. 3

| | |
|---|---|
| DP04.08 | **A) Controller**<br>The processes for handling the withdrawal of consent ensure that the processing activities concerned are discontinued.<br>If there is no other legal basis for the processing and the continued storage is not justified by another purpose, the personal data processed on the basis of the consent must be deleted. Appropriate processes must be implemented and documented for this, cf. the requirements in DP02.08, DP06.12.<br><br>**B) Processor**<br>The Processor assists the Controller as part of its obligation to follow instructions, if the Controller has expressly instructed the processor (cf. the requirements in DP07.04, DP07.10) that the processor is responsible for in ensuring that the processing activities are discontinued and the personal data are erased when consent has been withdrawn. If there is no corresponding instruction, this criterion is not applicable. If the processor has been instructed by the controller to handle withdrawals, it has implemented processes to ensure that the processing activities concerned are stopped and the PBD is deleted. These processes specifically stipulate the following:<br>• Responsibilities and communication channels regarding the handling of withdrawal requests and the execution of deletions<br>• Definition and concrete description of deletion mechanisms (documentation of individual processes and implementation requirements)<br>○ When defining the minimum requirements for deletion procedures, the specifications of the BSI IT-Grundschutz-Compendium CON.6 Deletion and destruction must be met<br>○ Responsibilities with regard to monitoring the deletion processes<br>○ Verification of the actual implementation and validity of the deletion<br>○ Definition of how deletions are documented<br>○ Inclusion of data deletion in backups and archives<br>○ Regular evaluation (at least annually) of the selected dele- |

| | |
|---|---|
| | tion mechanisms to determine whether they still correspond to the state of the art |

[GDPR] Art. 6 para. 1 lit. a, Art. 8

| | |
|---|---|
| DP04.06 | **A) Controller**<br>Where point (a) of Article 6 (1) GDPR applies (see the requirements in DP04.01 to DP04.08), in relation to the offer of information society services directly to a child, according to Art. 8 GDPR the processing of the personal data of a child shall be lawful where the child is at least 16 years old. If the child has not yet reached the age of sixteen, such processing is only lawful if and to the extent that this consent is given by or with the consent of the holder of parental responsibility for the child.<br>With regard to the general effectiveness of consent, the requirements in **DP04.01 to DP04.08** apply. In addition, it must be ensured that the choice of words, tonality and language style is adapted to the child target group. With regard to the specific conditions of Art. 8 GDPR, taking into account the available technology the controller must fulfill the following requirements<br>a) Evaluation whether the age of the minor using the information society service makes the consent or authorisation of the holder of parental responsibility unnecessary (age verification). For this purpose, appropriate processes must be implemented that take into account at least the following:<br>• Age verification systems must be implemented. It must be ensured that only the data that is absolutely necessary for age verification is processed.<br>• When selecting the respective age verification system, an assessment of the risk of the associated data processing must be carried out and documented.<br>• It must be ensured that the data obtained as part of the age verification process is not used for commercial purposes.<br>• If the child states that they have not yet reached the age limit (age of digital consent), the Controller can accept this information without further checks, but must ensure that the necessary consent or approval of the holder of parental responsibility has been obtained (see below).<br>b) If the child has not yet reached the age of 16, whether the required consent or authorisation for data processing has been given by the holder of parental custody and has actually been given by them (authentication). Appropriate processes must be implemented for this, which take into account at least the following:<br>• Confirmation by the child that its parents have given their consent is not sufficient, instead, measures for age verification must be implemented.<br>• Taking into account the available technology, the appropriateness and the risks associated with the processing (see risk assessment), the Controller must have implemented measures with regard to obtaining consent from the holder of parental responsibility or their consent. Appropriate measures must be implemented for this purpose (e.g. double opt-in procedure, a |

document signed by the parents (by post, fax, electronic scan), use of the parents' credit cards to legitimise transactions, telephone call or video conference with the parents on a toll-free number, etc.).

- When selecting the respective measures, it must be ensured that only the data that is absolutely necessary for this purpose is processed.
- The processes and implemented measures must be continuously reviewed. Controllers must be defined for this purpose.
- It must be ensured that Consent or the declaration of consent is given before data processing begins.
- In accordance with Art. 7 para. 3 sentence 3 GDPR, the Controller must inform the child of the consent given by the holder of parental responsibility. Appropriate processes must be implemented for this (Controller, communication channels).
- Once the child has reached the age of digital consent, consent to the processing of personal data by the holder of parental responsibility can be confirmed, amended or withdrawn by the child themselves. The Controller must inform the child of this once the age limit has been reached and request that the child take appropriate action. The child must be informed that they have the option to withdraw consent in accordance with Art. 7 para. 3 GDPR. In addition, the child must be informed of the right to be forgotten in accordance with Art. 17 GDPR. Appropriate processes must be implemented and documented for this purpose (Controller, processes regarding the verification of the age limit, communication channels, determination of the further procedure if the child does not take the required action).

The results of the inspection must be documented.

The specification of the individual requirements can be found in the evaluation notes.

**B) Processor**

In the case of an information society service offered directly to a child, the processing of the child's personal data is lawful if the child has reached the age of sixteen and the child has given consent to the processing. If the child has not yet reached the age of sixteen, such processing is only lawful if and to the extent that this consent is given by or with the consent of the holder of parental responsibility for the child. The Processor supports the Controller as part of its obligation to follow instructions in the fulfilment of the above conditions for a child's consent in relation to information society services.

In this context, the processor provides the controller with either a template for obtaining a child’s consent or a guidance document on formulating consent in accordance with Art. 8 para. 1 GDPR. With regard to the general effectiveness of consent, the requirements in **DP04** apply. If the processor is obliged by instruction from the controller to obtain consent itself in accordance with Art. 8 para. 1 GDPR, all requirements under section *A) Controller* must be fulfilled and proved by the processor.

## DP05 Processing of special categories of personal data

[GDPR] Art. 9 para. 1, 2 possibly in conjunction with state or federal standards, such as [BDSG] §§ 22, 27 para. 1

| | |
|---|---|
| DP05.01 | **A) Controller**<br>In addition to the requirements specified in DP03 and DP04, the following requirements must be fullfield when processing 'special categories of personal data' (SCPD):<br>1. The data subject has expressly consented to the processing of the aforementioned personal data for one or more specified purposes, unless under European Union or German law the prohibition under Art. 9 para. 1 GDPR cannot be lifted by the consent of the data subject (Art. 9 para. 2 lit. a GDPR)<br>In addition to the requirements for consent in accordance with Art. 7 GDPR (see DP04), explicit consent must explicitly refer to the processing of special categories of personal data and specifically name the data used and the purpose of use. An implied or tacit declaration is not permitted.<br>2. the processing is necessary for the Controller or the data subject to exercise the rights and fulfil the obligations arising from labour law and social security and social protection law, insofar as this is permitted under European Union law or German law or a collective agreement under German law which provides for appropriate safeguards for the fundamental rights and interests of the data subject (Art. 9 para. 2 lit. b GDPR).<br>With regard to the scope of processing, the Controller must first check and document whether a processing requirement arises from specific EU or national standard, e.g. for the purposes of pension and social security, health insurance, social assistance, housing, family or education support, which must be anchored in the respective special laws. This may also include works agreements and collective labour agreements.<br>3. Processing is necessary in order to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent (Art. 9 para. 2 lit. c GDPR).<br>When examining the applicability of lit. c, the Controller must ensure that obtaining consent proves to be (de facto) impossible, e.g. because the data subject is unconscious or cannot be reached due to physical absence and the processing obviously cannot be based on another legal basis.<br>4. the processing is carried out on the basis of appropriate safeguards by a foundation, association or other non-profit organisation with a political, philosophical, religious or trade union aim in the course of its legitimate activities and provided that the processing relates solely to the members or former members of the organisation or to persons who have regular contact with it in connection with its purpose of activity and the personal data are not disclosed externally without the consent of the data subjects (Art. 9 para. 2 lit. d GDPR). |

| | |
|---|---|
| | The Controller must ensure that the processing is carried out within the framework of the purpose of the respective organisation and on the basis of appropriate safeguards, including in particular technical and organisational measures (cf. DP08). It must be checked whether the processing includes appropriate activities that are necessary for the specific orientation of the organisation. The processing may only relate to the organisation's own members, former members and persons who are in regular contact with the organisation in relation to its respective purpose. Personal data may only be disclosed externally with the express consent of the data subjects.<br>5. the processing relates to personal data which the data subject has manifestly made public (Art. 9 para. 2 lit. e GDPR).<br>It must be ensured that the publication is due to a conscious act of will on the part of the data subject, i.e. that the publication undoubtedly originates from the data subject or was clearly initiated by them. The Controller must be able to demonstrate that the personal data has obviously been made public.<br>6. processing is necessary for the establishment, exercise or defence of legal claims or for the exercise of judicial proceedings (Art. 9 para. 2 lit. f GDPR).<br>The Controller must document why there is a need for the processing of PD for the exercise or defence of legal claims. Arbitrary disclosure of special categories of personal data that are not related to the content of the dispute is not permitted.<br>7. processing is necessary for reasons of substantial public interest on the basis of European Union or German law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Art. 9 para. 2 lit. g GDPR)<br>The Controller must document whether and which significant public interest exists. It must be ensured that the processing is proportionate, that the measures are therefore suitable and necessary to achieve the objective and that the disadvantages for the data subject are proportionate to the objective.<br>8. processing is necessary for the purposes of preventative or occupational medicine, for the assessment of an employee's fitness for work, for medical diagnosis, for the provision of health or social care or treatment, or for the management of health or social care systems and services on the basis of European Union or German law or a contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (Art. 9 para. 2 lit. h GDPR)<br>The Controller must explain on what legal basis such processing is authorised under European Union or German law or under a contract with a healthcare professional (e.g. doctors, medical staff).<br>The Controller must also ensure that the processing is necessary for the purposes mentioned in para. 2 lit. h GDPR "in the interest of individual natural persons and of society as a whole". Furthermore, processing is only permitted if it is carried out by specialised personnel or under their responsibility and this specialised personnel is subject to |

| | |
|---|---|
| | professional secrecy by law or the processing person is otherwise subject to a duty of confidentiality under European Union law, the German law or the regulations of a national competent authority.<br>9. Processing is necessary for reasons of public interest in the area of public health, such as the protection against serious cross-border threats to health or to ensure high standards of quality and safety of healthcare and of medicinal products and medical devices, on the basis of European Union law or German law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Art. 9 para. 2 lit. i GDPR). The Controller must document which standard under EU or German law legitimises the processing of special categories of personal data for the purposes referred to in point (i).<br>10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89 para. 1 on the basis of EU or German law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject (Art. 9 para. 2 lit. j GDPR).<br>The Controller must document which norm of European Union law or German law it refers to and must ensure that the requirement of a public interest refers to all alternatives mentioned in lit. j.<br>The specification of the individual requirements can be found in the test notes.<br><br>**B) Processor**<br>As part of its obligation to follow instructions, the processor supports the Controller in obtaining consent, if the Controller has expressly instructed the processor (cf. the requirements in **DP07.04, DP07.10**) that the processor is re-sponsible for obtaining consent from the data subjects on behalf of the controller. If there is no corresponding instruction, this criterion is not applicable. The content of the consent declaration is the responsibility of the controller and must be implemented by the processor. The Processor has to inform the controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions. The responsibilities and communication channels for this must be documented. |

[GDPR] Art. 9 para. 3, if applicable in conjunction with state or federal standards, such as [BDSG] §§ 22, 27 para. 1 in conjunction with [BDSG]

| | |
|---|---|
| DP05.02 | **A) Controller**<br>If special categories of personal data are processed for the purposes of Art. 9 para. 2 lit. h GDPR, the controller stipulates that these data are processed by **specialised personnel** or under their responsibility and that this specialised personnel or other persons processing the data are subject to a legal professional secrecy.<br>Data processing must be necessary on the basis of a contract with a healthcare professional.<br><br>**B) Processor**<br>If special categories of personal data are processed for the purposes of Art. 9 para. 2 lit. h GDPR the processor stipulates that this data is processed by **specialised personnel** or under their responsibility and this specialised personnel or other persons processing the data are subject to a legal professional secrecy. The processor must demonstrate to the Controller that all persons involved in the commissioned processing activities are subject to professional secrecy and that all persons are bound to maintain professional secrecy. |

| | |
|---|---|
| DP05.03 | **Controller and Processor**<br>If **genetic, biometric or health data are processed**, the processing may be governed separately by national regulations.<br>The controller must check and document whether such German regulations are relevant and which further conditions and restrictions result from them with regard to the processing of genetic, biometric or health data. The controller must document which standard they are referring to.<br>The further conditions, including the restrictions resulting from the national regulations, must be fulfilled.<br>The processing of genetic, biometric or health data must be carried out for the processing purposes specified in the national regulation.<br>The specification of the individual requirements can be found in the evaluation note. |

## DP06 Rights of data subjects

[GDPR] Art. 12 para. 1

| | |
|---|---|
| DP06.01 | **A) Controller**<br>Appropriate measures are taken to provide data subjects with information referred to in Art. 13, 14 and communication under Art. 15 to 22 and Art. 34 GDPR:<br>1. in a concise, transparent, intelligible and easily accessible manner<br>• The data protection information is clearly separated from other information that does not relate to data protection, e.g. contractual provisions, general terms and conditions of use<br>• The data protection information is understandable for a typical member of the target audience (taking into account the level of understanding of the persons concerned).<br>• It is immediately apparent to the data subject where and how they can access the data protection information (easy accessibility)<br>• If the controller's target audience is children or the goods/services are used by children in particular, the choice of words, tone and style of language is adapted to the child target group<br>• The controller actively provides the information in accordance with Art. 13 and 14 GDPR to the data subjects or directs the data subjects directly to the place where the information is available. The data subject has permanent access to the information in accordance with Art. 13 and 14 GDPR<br>• The controller reminds the data subject at regular intervals (at least annually) of the data protection declaration/information and where it can be found<br>• A common term is used, such as “data protection”, “data protection provisions”, “data protection information”, “data protection notice”<br>• In the case of complex, technical or unexpected processing operations, in addition to providing the information required under Art. 13 and 14 GDPR, a separate and clearly formulated description of the main consequences of the processing is provided<br>• The controller makes a documented assessment of whether there are any particular risks for the data subjects affected by the processing that should be brought to the attention of the data subjects. If this is the case, the data subjects is informed of these risks<br>• Use of multi-level privacy statements/information that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice<br>2. clear and plain language<br>• The information is provided in as simple a manner as possible, avoiding complex sentence and linguistic structures<br>• Abstract and ambiguous terms or room for interpretation are avoided.<br>• Modal verbs and words such as “can”, “could”, “some”, ‘often’ and “possible” are avoided |

| | |
|---|---|
| | • Paragraphs and sentences are well-structured and hierarchical relationships are shown with bullet points and indents.<br>• The information is written in the active rather than the passive voice and excessive nouns are avoided<br>• The information does not contain a disproportionate amount of legal, technical or specialized wording or terminology<br>• If the target audience of the data subjects is children, the choice of words, tone and style of language is adapted to the child target group so that the child recipient of the information also recognizes that the message/information is addressed to them<br>• Information is provided in the national language of the respective target group, i.e. in German<br><br>3. in writing or by other means, including, where appropriate, by electronic means<br>• The provision of information pursuant to Art. 13 and 14 GDPR and all notifications pursuant to Art. 15 to 22 and Art. 34 GDPR is made in writing or in another form, if necessary also electronically<br>• If the data subject has made the request to exercise their rights in electronic form, communication will take place electronically wherever possible, unless the data subject requests a different means of communication.<br>• The information pursuant to Art. 13 and 14 GDPR may also be provided in electronic form (e.g. also contextual “just-in-time pop-up notices”, 3D touch notices and data protection dashboards, videos and smartphone or IoT voice messages, if applicable, in addition to multi-level data protection information/notices)<br>• In the event that a website is operated: Use of multi-level privacy statements/notices that allow data subjects to go directly to specific points instead of displaying the entire information on the screen in the form of a single notice. Furthermore, when using multi-level privacy statements/information, the following must be ensured:<br>○ The information pursuant to Art. 13 and 14 GDPR is also made easily accessible in a single place or in a single document (digital or paper format)<br>○ The design and organization of the first level of the multi-level data protection information/notice must provide the data subject with an overall view of the information available to them regarding the processing of their personal data and indicate where/how they can find the individual information at the respective levels of the data protection information/notice.<br>○ The information contained at the different levels of a multi-level notice is consistent and does not differ in a contradictory manner from level to level<br>○ The first level of multi-level data protection information / notices contains information on the purposes of processing, the identity of the controller and the data subject: processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that will have the most significant impact on the data subject and the processing operations that the data subject may not expect<br>○ The above information will be brought to the attention of the |

| | |
|---|---|
| | data subject directly at the time the personal data is collected, e.g. by displaying it on the screen while the data subject is filling out an online form<br>○ With regard to the use of the multi-level approach in a non-digital environment: At the first level, at least the following information is communicated to the data subjects: Processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that has the most impact on the data subject and the processing operations that the data subject may not expect. It must be specified and documented how the further information required under Art. 13 and 14 GDPR is to be communicated<br>• If requested by the data subject, the information pursuant to Art. 13 and 14 and all notifications pursuant to Art. 15 to 22 and Art. 34 may be provided orally. However, with regard to the exercise of the data subject's rights under Art. 15 to 22 GDPR, the identity of the data subject must be proven in another form. The controller must specify how such proof of identity can be provided<br>○ In the case of oral provision of the information pursuant to Art. 13 and 14 GDPR by means of message recording, the controller enabled the data subject to listen to the recorded message several times<br>○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br><br>• The controller can provide the information in accordance with Art. 13 and 14 GDPR in combination with standardized icons<br>○ The icons used must be standardized<br>○ The icons are used in addition to the written data protection information<br>○ If the icons are provided in electronic form, they must be machine-readable<br>4. free of charge<br>• the controller does not charge a fee for the provision of information in accordance with Art. 13 and 14 GDPR or for notifications and measures taken in accordance with Art. 15 to 22 and Art. 34 GDPR<br>• The provision of information is not dependent on a financial transaction by the data subject<br>• Only in the case of manifestly unfounded or excessive requests from a data subject, particularly where they are repetitive, may the controller either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or b) refuse to act on the request. In such cases, the controller must provide evidence of the manifestly unfounded or excessive nature of the request.<br>• The Controller must document which modalities and formats are used for the transmission of information in accordance with Art. 13 and 14 GDPR<br>• The following deadlines are observed with regard to the time of notification of the information in accordance with Art. 13 and 14 GDPR: |

| | |
|---|---|
| | a) PBD is collected from the data subject themselves<br>• The information (data protection information) is transmitted before the personal data is collected, see Art. 13 para. 1 GDPR<br>b) Personal data is not collected from the data subject<br>• With regard to the timing of the information to the data subject, the following deadlines must be observed in accordance with Art. 14 para. 3 GDPR:<br>o The information (data protection information) is communicated to the data subject within a reasonable period of time after obtaining the personal data "taking into account the specific circumstances of the processing of the personal data", at the latest within one month (= maximum period) (Art. 14 para. 3 lit. a GDPR). With regard to the deadline, the following restrictions must be observed and earlier provision of the information must be ensured accordingly.<br>o If the personal data is used to communicate with the data subject: The information must be provided at the latest at the time of the first communication with the data subject (even if the latest deadline has not yet expired) (Art. 14 para. 3 lit. b GDPR)<br>o If disclosure of the personal data to another recipient is intended: The information must be provided at the latest at the time of this disclosure (even if the latest deadline has not yet expired) (Art. 14. para. 3 lit. c GDPR)<br>o When deciding when to provide the information in accordance with Art. 14 GDPR, the legitimate expectations of the data subjects (what is the data subject's interest in being informed, i.e. how urgently is the information needed to exercise their rights), the potential impact of the processing on the latter and their ability to exercise their rights in relation to this processing must always be taken into account. The reasons for the decision as to why the information was provided at the specific time chosen must be documented by the controller. In accordance with the principle of good faith, the information must be provided as early as possible before the expiry of the specified deadlines<br>• The information obligation pursuant to Art. 14 para. 1 to 4 GDPR does not apply in the following cases, cf. Art. 14 para. 5 GDPR:<br>o The data subject already has the information. The controller must prove which information is already available, how and when it received it, and that this information has not been subject to any significant changes in the meantime. Non-material changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors.<br>o The provision of information proves to be legally or factually impossible or requires a disproportionate effort. The impossibility of providing information applies in particular to cases in which the controller does not know the data subject and therefore cannot inform the person. The controller must explain the factors that prevent it from providing the data subject with the information in question. When assessing whether the effort is disproportionate, the controller must weigh up the effort involved in providing the information against the interests of the data subject and document the |

| | |
|---|---|
| | result<br>○ There is still no obligation to provide information if the processing is carried out for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. However, the prerequisite for this is that the conditions and guarantees specified in Art. 89 para. 1 GDPR are met. It must be ensured that technical and organizational measures are in place, in particular to ensure compliance with the principle of data minimization. Pseudonymization may also be one of the appropriate measures, provided that it is possible to achieve these purposes in this way<br>• If the information pursuant to Art. 13 and 14 GDPR is changed significantly or factually (in particular in the event of a change in the purpose of processing, the identity of the controller, a change in the way in which the data subjects can exercise their rights with regard to processing, an extension of the categories of recipients, future transfer to a third country), the data subjects must be informed of the changes in good time before they actually take effect (at least 14 days in advance). There is no obligation to inform in the case of non-material changes. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors. The controller must ensure that the changes are communicated in a way that ensures that the majority of recipients actually pay attention to them. With regard to changes to the information in accordance with Art. 13 and 14 GDPR, the controller has implemented and documented processes which, in particular, make provisions for:<br>○ Specifications regarding the review and recording of any adaptation requirements for data protection information in the event of changes to processing activities (definition of responsibilities, communication channels, involvement of the data protection officer, documentation of adaptation requirements, sensitization of employees)<br>○ Definition of responsibilities for making, approving and publishing changes to the data protection information<br>○ Determine how the changes will be communicated<br>- It must be ensured that the majority of recipients take note of the notification of changes (e.g. by email, by traditional letter on paper, by pop-up on a website or in another way that effectively brings the changes to the attention of the data subject<br>- The notification of changes must be separate from other information<br>- intelligible and easily accessible form, using clear and plain language, see **DP06.01**<br>- The data subject is informed of the possible effects of these changes.<br>• With regard to the exercise of data subject rights pursuant to Articles 15 to 22 GDPR, the implemented processes take into account the following deadlines.<br>○ The controller provides the data subject with information on the measures taken pursuant to Articles 15 to 22 GDPR without undue |

| | |
|---|---|
| | delay and in any event within one month of receipt of the data subject's request. A possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR will also be taken into account in the process if this is necessary, taking into account the complexity and number of requests. The data subject will be informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, it informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.<br>• Every request received and its processing must be documented by the controller.<br>If the obligations pursuant to Art. 12 to 22 and Art. 34 GDPR and Art. 5 GDPR are not fulfilled by the controller pursuant to Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of rights and obligations.<br><br>**B) Processor**<br>Pursuant to Art. 28 para. 3 sentence 2 lit. e GDPR, the Processor must support the Controller, as far as possible and as part of its obligation to follow instructions with appropriate technical and organisational measures to comply with the obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III GDPR.<br>The details of the support to be provided by the Processor must be set out in the data processing agreement or in an annex to this agreement. The support service includes, in particular, the provision of Information and documents that the Controller can use to respond to requests.<br>As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 12 para. 3

| | |
|---|---|
| **DP06.02** | **A) Controller**<br>The Controller has documented processes for providing information to the data subject on the measures it has taken on the basis of a data subject request in accordance with Art. 15 - 22 GDPR. The processes take into account in particular:<br>• The procedure for checking whether the requesting person's personal data is being processed and the provision of information must be defined, naming the respective bodies involved. |

| | |
|---|---|
| | • Sensitization of employees regarding the handling of requests from data subjects<br>• Absence and substitution rules have been established to ensure compliance with existing deadlines<br>• Responsibilities for reviewing the data subject request must clearly define responsibilities for the provision of information and regulations for the communication channels with the data subjects. When selecting communication channels, it must be ensured that data is transmitted securely (e.g. via end-to-end encrypted e-mail or with the help of encrypted documents, use of a document exchange platform).<br>• Determining how communication with the data subject will take place: If the data subject has made the request in electronic form, communication is carried out electronically wherever possible, unless the data subject requests a different means of communication.<br>  ○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>  ○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• It is ensured that all employees at the Controller recognise data subject enquiries as such, regardless of the channel of receipt, and that everyone is aware of the process for dealing with such enquiries.<br>• Definition of how incoming data subject requests are documented.<br>• Determining how long data subject inquiries are stored and informing the inquirer about this storage period.<br>• Consideration of the authentication of data subjects, cf. **DP06.03**<br>• Responsibilities must be defined with regard to monitoring compliance with the processing time and quality<br>• The process must take into account that if no PD of the requestor is processed, negative information is issued, cf. **DP06.09**.<br>• It must be ensured that the exercise of rights by data subjects does not adversely affect the rights and freedoms of other persons. Appropriate checks have been established for this purpose, including the definition of responsibilities and the definition of how certain information may be made unidentifiable. Where necessary, information is made unidentifiable (e.g. redaction) to protect the rights and freedoms of other persons<br>• The implemented processes take into account the following deadlines:<br>  ○ The controller provides the data subject with information on the measures taken in accordance with Articles 15 to 22 GDPR without undue delay and in any event within one month of receipt of the data subject's request. A possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR will also be taken into account in the process if this is necessary, taking into account the complexity and number of requests. |

The data subject will be informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, he informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.

- Every request is received and its processing is documented by the Controller.
- The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**.
- Sample documents are available for responding to requests from data subjects.
- The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests from a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the controller must provide evidence of the manifestly unfounded or excessive character of the request

If the obligations under Art. 12 to 22 GDPR are not fulfilled by the controller pursuant to Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. 12 to 22 GDPR.

**B) Processor**

Pursuant to Art. 28 sec. 3 sentence 2 lit. e GDPR, the Processor must support the Controller as far as possible and as part of its obligation to follow instructions, to inform the data subject of the measures taken in response to the request pursuant to Art. 15 - 22 GDPR.

If the data subject's request concerns personal data to which the Processor can only grant access, the Processor must provide a contact point to ensure that the request is implemented.

Details on the Processor's obligation to provide support in the course of processing requests in accordance with Art. 15 - 22 GDPR can be found in **DP06.08, DP06.09, DP06.11, DP06.12, DP06.13, DP06.14, DP06.15, DP06.16, DP06.17**.

The Processor acts within the scope of its authorisations arising from the underlying data processing agreement. The Processor documents the instructions received from the Controller and the support services provided.

As part of the support function, the Processor designates a contact person

| | |
|---|---|
| | for the Controller. |

[GDPR] Art. 12 in particular para. 6

| | |
|---|---|
| DP06.03 | **A) Controller**<br>Processes have been implemented that enable secure and data-saving **authentication of the data subjects** in the context of requests according to Article 15 – 21 GDPR.<br>The processes are at least subject to the following regulations:<br>• Responsibilities for carrying out authentication<br>• Training of employees with regard to the authentication of persons authorised to receive information<br>• In the event of enquiries from third parties on behalf of the data subject: ensure that the authorisation also relates to obtaining information under data protection law. Appropriate work instructions must be documented for this purpose.<br>• If there are reasonable doubts about the identity of the natural person, the controller must request additional information to confirm the identity of the data subject. It must be determined what additional information must be requested.<br>• Determination of the authentication method, taking into account the risk to the rights and freedoms of the data subjects (e.g. request for additional information, transmission of an identification document, identification via eIDAS service, postal/video identification, identification via user account) with corresponding work instructions. It must be ensured that the principle of data minimisation pursuant to Art. 5 para. 1 lit. c GDPR.<br>• Documentation of the type and date of authentication of the applicant<br><br>**B) Processor**<br>If required, the processor supports the controller as part of its obligation to follow instructions to authenticate the data subject in the context of requests according to Article 15 – 21 GDPR.<br>In this context, the processor forwards any requests according to Articles 15 – 21 GDPR to the controller and inform the data subject thereof.<br>If the processor is obliged by instruction from the controller to carry out the authentication of the data subjects in the course of an request in accordance with Articles 15 - 21 GDPR partly or completely, the processor must have established processes for authentication, which in particular specify: Responsibilities for performing authentication, training of employees with regard to the authentication of persons entitled to information, determination of the authentication method taking into account the risk to the rights and freedoms of the data subjects, documentation of the type and date of authentication of the data subject. As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 13 para. 1, 2, 4

| | |
|---|---|
| DP06.04 | **A) Controller**<br>When the PD is collected **directly from the data subject,** the following information is communicated to the data subject before collection in accordance with Art. 13 GDPR:<br>1. name and contact details of the Controller and, if applicable, his representative (Art. 13 para. 1 lit. a GDPR),<br>2. Contact details of the data protection officer, if applicable (Art. 13 para. 1 lit. b GDPR),<br>3. purposes and legal basis of the processing (Art. 13 para. 1 lit. c GDPR),<br>4. where applicable, legitimate interests of the Controller or a third party (Art. 13 para. 1 lit. d GDPR),<br>5. where applicable, Recipients or categories of recipients of the PD (Art. 13 para. 1 lit. e GDPR),<br>6. where applicable, the Controller's intention to transfer the personal data to a third country or an international organisation (Art. 13 para. 1 lit. f GDPR),<br>7. duration of storage of the personal data or, if not possible, the criteria for determining this duration (Art. 13 para. 2 lit. a GDPR),<br>8. existence of the right to request (Art. 13 para. 2 lit. b GDPR),<br>9. the existence of a right to rectification, erasure or restriction of processing or a right to object to processing (Art. 13 para. 2 lit. b GDPR),<br>10. existence of the right to data portability (Art. 13 para. 2 lit. b GDPR),<br>11. where applicable, the existence of the possibility to withdraw consent (Art. 13 para. 2 lit. c GDPR),<br>12. existence of the right to lodge a complaint and indication of the supervisory authority (Art. 13 para. 2 lit. d GDPR),<br>13. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data (Art. 13 para. 2 lit. e GDPR),<br>14. the existence of automated decision-making, including profiling, referred to in Art. 22 para. 1 and 4 GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art. 13 para. 2 lit. f GDPR).<br>• The information (data protection information) is provided before the PBD is collected, see Art. 13 para. 1 GDPR.<br>• The information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in DP06.01, cf. DP06.01<br>• The data protection information is clearly separated from other information that does not relate to data protection, e.g. contractual provisions, general terms of use<br>• The information is provided in the national language of the respective |

| | |
|---|---|
| | target group, i.e. in German<br>• If the controller's target audience is children or the goods/services are used by children in particular, the choice of words, tone and language style must be adapted to the child target group<br>• The controller actively provides the information in accordance with Art. 13 GDPR to the data subjects or directs the data subjects directly to the place where the information is available<br>• The data subject has permanent access to the information in accordance with Art. 13 GDPR<br>• The controller reminds the data subject at regular intervals (at least once a year) of the privacy policy/information and where it can be found<br>• A common term is used, such as “data protection”, “data protection provisions”, “data protection information”, “data protection notice”<br>• In the case of complex, technical or unexpected processing operations, in addition to providing the information required under 14 GDPR, a separate and clearly formulated description of the main consequences of the processing is provided<br>• Use of multi-level data protection declarations/information that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice.<br>• The information is provided is provided in writing or by other means, including, where appropriate, by electronic means<br>○ The provision can also take place in electronic form (e.g. also context-related “just-in-time pop-up notices”, 3D touch notices as well as data protection dashboards, videos and smartphone or IoT voice messages in addition to multi-level privacy statements/notices)<br>○ In the event that a website is operated: Use of multi-level data protection information/notices that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice. Furthermore, when using multi-level privacy statements/information, the following must be ensured:<br>○ The information pursuant to Art. 13 GDPR is also provided in an easily accessible manner in a single location or in a single document (digital or paper format).<br>○ The design and structure of the first level of the multi-level data protection information/notice must provide the data subject with an overview of the information available to them regarding the processing of their personal data and show where/how they can find the individual information at the respective levels of the data protection declarations/information.<br>○ The information contained at the different levels of a multi-level notice is consistent and does not differ in a contradictory manner from level to level<br>○ The first level of multi-level data protection information notice contains information on: the purposes of the processing, the identity of the controller and a description of the data subject's |

rights, information about the processing that has the most impact on the data subject and the processing operations that the data subject may not expect o The above information is consistent and not contradictory from level to level. not expected by the data subject

- The above information will be brought to the attention of the data subject directly at the time of collection of the personal data, e.g. by displaying it on the screen while the data subject fills out an online form
- With regard to the use of the multi-level approach in a non-digital environment: At the first level, at least the following information will be communicated to the data subjects: Processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that has the greatest impact on the data subject and the processing operations that the data subject may not expect. It must be determined and documented how the further information required under Art. 13 GDPR is communicated
- If requested by the data subject, the information pursuant to Art. 13 GDPR may be provided orally. The controller must determine how a corresponding proof of identity can be provided.
  - In the case of the oral provision of information pursuant to Art. 13 GDPR by means of message recording, the controller enables the data subject to listen to the recorded message several times
  - The controller documents: the desire for information in oral form, the fact that the information was provided to the data subject
- The controller may provide the information pursuant to Art. 13 GDPR in combination with standardized icons. Art. 13 GDPR in combination with standardized icons
  - The icons used must be standardized
  - The icons are used in addition to the written data protection information
  - If the icons are provided in electronic form, they must be machine-readable

- The information is provided free of charge, see **DP06.01**

If the data subject already has the above-mentioned information, none of the information to be provided in paragraphs 1-3 must apply. In this case,. the principle of accountability requires that controllers demonstrate (and document) what information the data subject already has, how and when they received it and that non-substantial changes have since occurred to that information that would render it out of date. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors. The Controller informs data subjects of any changes to the information in accordance with Art. 13 GDPR.

If the information pursuant to Art. 13 is changed significantly or factually (in particular in the event of a change in the purpose of processing, the identity of the controller, a change in the way in which the data subjects can exercise their rights with regard to processing, an extension of the

| | |
|---|---|
| | categories of recipients, future transfer to a third country), the data subjects will be informed of the changes in good time before they actually take effect (at least 14 days in advance). There is no obligation to inform in the case of non-material changes. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors. The controller must ensure that the changes are communicated in a way that ensures that the majority of recipients actually pay attention to them. With regard to changes to the information in accordance with Art. 13, the controller has implemented and documented processes which, in particular, make provisions for:<br>• Specifications regarding the review and recording of any adaptation requirements for data protection information in the event of changes to processing activities (definition of responsibilities, communication channels, involvement of the data protection officer, documentation of adaptation requirements, sensitization of employees)<br>• Definition of responsibilities for making, approving and publishing changes to the data protection information<br>• Determine how the changes are to be communicated:<br>  ○ It must be ensured that the majority of recipients are aware of the change notification (e.g. by e-mail, by traditional letter on paper, by pop-up on a website or in any other way that effectively brings the changes to the attention of the data subject<br>  ○ The notification of changes must be made separately from other information<br>  ○ The information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, see DP06.01<br>  ○ The possible effects of these changes are explained to the data subject<br><br>**B) Processor**<br>In accordance with Art. 28 para. 3 sentence 2 lit. e GDPR, the Processor supports the Controller as far as possible and as part of its obligation to follow instructions in ensuring that the information pursuant to Art. 13 GDPR can be communicated to the data subjects of the IPS.<br>In this context, the Processor must provide the Controller with the necessary information on data processing in the context of the IPS and demonstrate in its documentation that internal processes are in place to provide support with the Information to be provided. The process documentation must indicate which internal departments are involved in the support obligation and serve as a point of contact for the Controller. The Processor must document support services provided or log user actions if instructions are implemented automatically. |

[GDPR] Art. 14 para. 1,2

| | |
|---|---|
| **DP06.05** | **A) Controller** |

| | |
|---|---|
| | If PD is **not** collected **directly from the data subject**, the following information must be made available to the data subject:<br>1. name and contact details of the Controller and, if applicable, his representative (Art. 14 para. 1 lit. a GDPR),<br>2. Contact details of the data protection officer (Art. 14 para. 1 lit. b GDPR),<br>3. purposes and legal basis of the processing (Art. 14 para. 1 lit. c GDPR),<br>4. categories of personal data that are processed (Art. 14 para. 1 lit. d GDPR),<br>5.Recipients or categories of recipients of the PD, if applicable (Art. 14 para. 1 lit. e GDPR),<br>6. If applicable, the Controller's intention to transfer the personal data to a third country or an international organisation (Art. 14 para. 1 lit. f GDPR),<br>7. duration of storage of the personal data or, if not possible, the criteria for determining this duration (Art. 14 para. lit. a GDPR),<br>8. legitimate interests of the Controller or a third party (Art. 14 para. 2 lit. b GDPR),<br>9. existence of the right to request (Art. 14 para. 2 lit. c GDPR),<br>10. the existence of a right to rectification, erasure or restriction of processing or a right to object to processing (Art. 14 para. 2 lit. c GDPR),<br>11. existence of the right to data portability (Art. 14 para. 2 lit. c GDPR),<br>12. the existence of the possibility of withdrawal of consent (Art. 14 para. 2 lit. d GDPR),<br>13. existence of the right to lodge a complaint and indication of the supervisory authority (Art. 14 para. 2 lit. e GDPR),<br>14. source of the personal data (Art. 14 para. 2 lit. f GDPR),<br>15. the existence of automated decision-making, including profiling, referred to in Art. 22 para. 1 and 4 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject(Art. 14 para. 2 lit. g GDPR).<br>• The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>• The data protection information is clearly separated from other information that does not relate to data protection, e.g. contractual provisions, general terms of use<br>• If the controller's target audience is children or the goods/services are used by children in particular, the choice of words, tone and style of language must be adapted to the child target group<br>• The controller actively provides the information in accordance with Art. 14 GDPR to the data subjects or directs the data subjects directly to the place where the information is available<br>• The information is provided in the national language of the respective target group, i.e. in German |

| | |
|---|---|
| | • The data subject has permanent access to the information in accordance with Art. 14 GDPR<br>• The controller reminds the data subject at regular intervals (at least annually) of the privacy policy/information and where it can be found<br>• A common term is used, such as “data protection”, “data protection provisions”, “data protection information”, “data protection notice”<br>• In the case of complex, technical or unexpected processing operations, in addition to providing the information required under 14 GDPR, a separate and clearly formulated description of the main consequences of the processing is provided<br>• Use of multi-level data protection information/notice that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice.<br>  • The information is provided is provided in writing or by other means, including, where appropriate, by electronic means<br>  ○ The information can also be provided in electronic form (e.g. also context-related “just-in-time pop-up notices”, 3D touch notices as well as data protection dashboards, videos and smartphone or IoT voice messages in addition to multi-level data protection information statements/notices)<br>  ○ In the event that a website is operated: Use of multi-level data protection information/notices that allow data subjects to directly access certain points instead of displaying the entire information on the screen in the form of a single notice. Furthermore, the use of multi-level privacy statements/information must be ensured.<br>  ○ The information pursuant to Art. 14 GDPR is also made easily accessible in a single location or in a single document (digital or in paper format).<br>  ○ The design and structure of the first level of the multi-level data portection information/notice must provide the data subject with an overall view of the information available to them regarding the processing of their personal data and indicate where/how they can find the individual information at the respective levels of the privacy notice/information.<br>  ○ The information contained at the different levels of a multi-level notice is consistent and does not differ in a contradictory manner from level to level<br>  ○ The first level of multi-level data protection information/notice contains information on: the purposes of the processing, the identity of the controller and a description of the data subject's rights, information about the processing that has the greatest impact on the data subject and the processing operations that the data subject may not expect o The above information will be brought to the attention of the data subject directly at the time of collection of the personal data. not expected by |

| | |
|---|---|
| | the data subject<br>○ The above information will be brought to the attention of the data subject directly at the time of collection of the personal data, e.g. by displaying it on the screen while the data subject fills out an online form<br>○ With regard to the use of the multi-level approach in a non-digital environment: At the first level, at least the following information will be communicated to the data subjects: Processing purposes, the identity of the controller and a description of the data subject's rights, information about the processing that has the greatest impact on the data subject and the processing operations that the data subject may not expect. It must be determined and documented how the communication of further information required under Art. 14 GDPR is carried out<br>○ If requested by the data subject, the information may be provided orally in accordance with Art. 14 GDPR. The controller must determine how a corresponding proof of identity can be provided.<br>▪ In the case of verbal provision of information pursuant to Art. 14 GDPR by means of message recording, the controller enables the data subject to listen to the recorded message several times<br>▪ The controller documents: the desire for information in oral form, the fact that the information was provided to the data subject<br>○ The controller may provide the information pursuant to Art. 14 GDPR in combination with standardized icons. Art. 14 GDPR in combination with standardized icons<br>▪ The icons used must be standardized<br>▪ The icons are used in addition to the written data protection information<br>▪ If the icons are provided in electronic form, they must be machine-readable<br>• The information is provided free of charge, see **DP06.01**<br><br>With regard to the time at which the data subject must be informed, the following deadlines are met in accordance with Art. 14 para. 3 GDPR:<br>• The above information must be provided to the data subject within a reasonable period of time after the personal data has been collected, “having regard to the specific circumstances in which the personal data are processed,” at the latest within one month (= maximum period) (Art. 14 para. 3 lit. a) GDPR). With regard to the deadline, the following restrictions must be observed and, accordingly, earlier disclosure of the information must be ensured.<br>○ If the personal data are to be used for communication with the data subject: The information must be provided at the latest at the time of the first communication with the data subject (even |

| | |
|---|---|
| | if the deadline has not yet expired) (Art. 14 para. 3 lit. b GDPR).<br>○ If a disclosure to another recipient is envisaged: The information must be provided at the latest when the personal data are first disclosed (even if the deadline has not yet expired) (Art. 14 para. 3 lit. c GDPR).<br>○ When deciding when to provide the information pursuant to Art. 14 GDPR, the legitimate expectations of the data subjects (what is the data subject's interest in the information, i.e. how urgently is the information needed to exercise their rights), the potential impact of the processing on them, and their ability to exercise their rights in relation to this processing must always be taken into account. The reasons for the decision to provide the information at the specific time chosen must be documented by the controller. In accordance with the principle of fairness, the information is provided as early as possible before the expiry of the specified deadlines.<br>The Information to be provided in accordance with Art. 14 para. 1 - 4 GDPR does not apply in the following cases, see Art. 14 para. 5 GDPR:<br>• The data subject already has the information. The controllers have to demonstrate (and document) what information the data subject already has, how and when they received it and that non-substantial changes have since occurred to that information that would render it out of date. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors.<br>• The provision of information proves to be legally or actually impossible or requires a disproportionate effort. The impossibility of providing information applies in particular to cases in which the Controller does not know the data subject and is therefore unable to inform the person. The Controller must document the reasons that prevent him from providing the information to the data subject. When assessing whether the effort involved is disproportionate, the Controller must weigh up the effort involved in providing the information against the interests of the data subject and document the result.<br>Furthermore, there is no information to be provided if the processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. However, the prerequisite for this is that the conditions and guarantees specified in Art. 89 para. 1 GDPR are met. It must be ensured that technical and organisational measures are in place to ensure, in particular, that the principle of data minimisation is respected. Pseudonymisation may also be one of the appropriate measures, provided that it is possible to fulfil these purposes in this way.<br>Obtaining or disclosing the personal data the processing of which must be relayed to the data subject in principle, is expressly regulated by German law or European Union law.<br>The information is subject to professional secrecy under the German law or of the European Union (e.g. a person bound to secrecy by law or professional regulations, e.g. a doctor, lawyer or |

| | |
|---|---|
| | tax consultant).<br>If the controller invokes an exception pursuant to Art. 14 para. 5 GDPR, the respective reasons for the existence of an exception must be documented.<br><br>If the information pursuant to Art. 14 is changed significantly or factually (in particular in the event of a change in the purpose of processing, the identity of the controller, a change in the way in which the data subjects can exercise their rights with regard to processing, an extension of the categories of recipients, future transfer to a third country), the data subjects will be informed of the changes in good time before they actually take effect (at least 14 days in advance). There is no obligation to inform in the case of non-substantial changes. Non-substantial changes are, for example, corrections of spelling mistakes or stylistic or grammatical errors. The controller must ensure that the changes are communicated in a way that ensures that the majority of recipients actually pay attention to them. With regard to changes to the information in accordance with Art. 14 GDPR, the controller has implemented and documented processes which, in particular, make provisions for:<br>• Specifications regarding the review and recording of any adaptation requirements for data protection information in the event of changes to processing activities (definition of responsibilities, communication channels, involvement of the data protection officer, documentation of adaptation requirements, sensitization of employees)<br>• Definition of responsibilities for making, approving and publishing changes to the data protection information<br>• Determine how the changes are communicated:<br>○ It must be ensured that the majority of recipients are aware of the notification of change (e.g. by email, by traditional letter on paper, by pop-up on a website or in another way that effectively brings the changes to the attention of the data subject<br>○ The notification of change must be separate from other information<br>○ The information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>○ The possible effects of these changes are explained to the data subject<br><br>**B) Processor**<br>In accordance with Art. 28 para. 3 sentence 2 lit. e GDPR, the Processor supports the Controller as far as possible and as part of its obligation to follow instructions in ensuring that the information pursuant to Art. 14 GDPR can be communicated to the data subjects of the IPS.<br>To this end, the Processor must provide the Controller with the necessary information on data processing in the context of IPS and demonstrate in its documentation that internal processes are in place to provide support |

| | |
|---|---|
| | with the information to be provided. The process documentation must indicate which internal departments are involved in the support obligation and serve as a point of contact for the Controller. The Processor must document support services provided or log user actions if instructions are implemented automatically.<br>As part of the support function, the Processor appoints a contact person for the Controller. |

[GDPR] Art. 13 para. 3, Art. 14 para. 4; [BDSG] § 32 para. 1, § 33 para. 1

| | |
|---|---|
| **DP06.06** | **A) Controller**<br>If the Controller intends to further process the PD for a purpose other than that for which the PD was collected,<br>• the Controller provides data subjects whose personal data is intended to be processed for a purpose other than the original purpose of collection with information in accordance with **DP06.04** or **DP06.05** and corresponding information on the other purpose<br>• documents a consideration in which it states that the processing for the other purpose is compatible with that for which the PD were originally collected, cf. requirement **DP03.08**<br><br>**B) Processor**<br>In the event of an extension of the purpose, the Processor must support the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in informing the data subject of this other purpose with all relevant information in accordance with the aforementioned criteria.<br>As part of the support function, the Processor appoints a contact person for the Controller. |

[GDPR] Art. 12 para. 3, Art. 15 para. 1, 2

| | |
|---|---|
| **DP06.07** | **A) Controller**<br>The data subject must be given confirmation as to whether or not personal data concerning him or her are being processed by the controller. In accordance with Art. 15 para. 1 GDPR the following information is shared with the data subject:<br>1. name and contact details of the Controller,<br>2. purposes of the processing (Art. 15 para. 1 lit. a GDPR),<br>3. categories of personal data processed (Art. 15 para. 1 lit. b GDPR),<br>4. recipients or categories of recipients of the personal data (Art. 15 para. 1 lit. c GDPR),<br>5. duration of storage of the personal data or, if not possible, the criteria for determining this duration (Art. 15 para. 1 lit. d GDPR),<br>6. the existence of the right to rectification and erasure of personal data concerning them or to restrict processing by the Controller or a right to object to such processing (Art. 15 para. 1 lit. e GDPR), |

| | |
|---|---|
| | 7. the existence of the right to lodge a complaint with a supervisory authority (Art. 15 para. 1 lit. f GDPR),<br>8. where the personal data are not collected from the data subject, any available information as to their source (Art. 15 para. 1 lit. g GDPR),<br>9. the existence of automated decision-making, including profiling, referred to in Art. 22 para. 1 and 4 GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art. 15 para. 1 lit. h GDPR).<br>If no personal data is processed, the requesting person has to be informed about that fact (cf. **DP 06.09**)<br>• The information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>• Sample documents are available for responding to requests from data subjects.<br>• The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the data controller must provide evidence of the manifestly unfounded or excessive character of the request.<br>• If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• The controller provides the information to the data subject without undue delay and in any case within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, the controller informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory |

| | |
|---|---|
| | authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.<br>• Every request and its processing is documented by the controller.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in providing information to data subjects about the PDP in accordance with Art. 15 para. 1 GDPR. In this context, the processor forwards any requests in accordance with Articles 15 - 21 GDPR to the controller and informs the data subject of this.<br>The service makes it easier for controllers to comply with the obligation to grant data subjects access to their PD in accordance with the information above.<br>The obligation to provide support can be fulfilled by the processor enabling the compilation of personal data technically, e.g., extraction option, interface for managing personal data.<br>As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 15 para. 3

| | |
|---|---|
| DP06.08 | **A) Controller**<br>A process is in place to support the provision of a **copy of the personal data undergoing processing**.<br>The process regulates at least:<br>1. Defined responsibilities, including deadlines and communication channels with regard to the creation and provision of the copy of the PD<br>2. Ensuring that the copy of the PD is complete, true to the original and comprehensible<br>3. determining how the copy of the PD is made available, e.g. through secure access. The following requirements must be implemented:<br>• Provision of the copy of the data in a tangible, durable form (text, electronic) so that the person can easily download it.<br>• The data subject must be provided with a faithful and comprehensible reproduction of the PD. A list of the PD in aggregated form is not sufficient if the context of the data processing is not clear. The data subject must be provided with extracts from documents or entire documents, as well as extracts from databases containing the PBD, if this is necessary to enable them to effectively exercise their data subject rights, in particular if data is generated from other data or if it is based on free fields and the provision of such a copy is necessary to enable the data subject to verify the accuracy and completeness of the data and to ensure the comprehensibility of the data. In doing so, the rights and freedoms of other persons must be taken into account (see No. 4). The controller must have established processes for verifying the scope of the data to be disclosed (responsibilities regarding the verification of the necessity |

| | |
|---|---|
| | and scope of the provision of a copy of the documents and extracts from databases, Sensitizing employees regarding the provision of copies of the PD).<br>• If the data subject submits the request electronically, the information must be provided in a commonly used electronic format, unless the data subject indicates otherwise.<br>• Written information, including in electronic form, is preferable to other forms.<br>• The format must enable the information to be presented in a comprehensible and easily accessible manner.<br>• In the case of electronic/digital transmission, the data subject must be able to download their data in a commonly used electronic format<br>• Secure transmission of data (e.g. via end-to-end encrypted e-mail or using encrypted documents, use of a document exchange platform) must be ensured.<br>4. Verification that the rights and freedoms of other persons are not impaired by the data copy, if necessary redaction<br>5. Free provision of the first copy of the PD<br><br>The controller provides the information to the data subject without undue delay and in any event within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, the controller informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR in the fulfillment of data subject rights within the scope of its obligation to follow instructions. In this context, the Processor forwards any requests for the provision of a copy to the Controller and informs the data subject of this. In addition, the obligation to provide support can be fulfilled by the processor enabling the provision of copies technically, e.g., by implementing an extraction option.<br>As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 15 para. 1, [BDSG] § 34

| | |
|---|---|
| DP06.09 | **A) Controller**<br>The controller has a process that informs potentially data subjects that no personal data is being processed.<br>The process applies in particular to specifications:<br>• Responsibilities with regard to the provision of negative information<br>• If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>  ○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>  ○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• Definition of how negative information is provided. Secure transmission of the data (e.g. by end-to-end encrypted email or using encrypted documents, use of a document exchange platform) must be ensured.<br>• Determining how long personal data that is processed in the context of the data subject's request and the provision of negative information is stored and informing the requesting party about this storage period.<br>If personal data relating to a data subject is processed, the information must be provided in accordance with Art. 15 para. 1 GDPR (cf. DP06.07).<br>• The controller provides the information to the data subject without undue delay and in any case within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, the controller informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in DP06.01Every request and its t processing is documented by the controller.Sample documents are available for responding to data subject requests.<br>• The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - ex- |

| | |
|---|---|
| | cessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the data controller must provide evidence of the manifestly unfounded or excessive character of the request.<br><br>**B) Processor**<br>The processor supports the controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as part of its obligation to follow instructions when providing information to a potential data subject that no personal data is being processed.<br>As part of the support function, the Processor designates a contact person for the Controller. |

[BDSG] § 34 para. 2

| | |
|---|---|
| DP06.10 | **Controller**<br>The **data stored for the purpose of providing information to the data subject and for the preparation of such information** may only be processed for this purpose and for the purposes of data protection monitoring; for other purposes, processing must be restricted in accordance with Art. 18 GDPR.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 16, Art. 17, Art. 18, Art. 19

| | |
|---|---|
| DP06.11 | **A) Controller**<br>A process is in place to accept and process **requests for rectification, erasure and restriction** from data subjects. The process for rectification, erasure and restriction of processing of the processed personal data includes<br>1. Processes for authentication of data subjects,<br>2. The controller must have established and documented processes for verifying the identity of the data subject (authentication), cf. the requirements in DP06.03<br>3. defined responsibilities for the processes to be carried out, including deadlines and communication channels<br>4. absence and substitution rules have been established to ensure compliance with existing deadlines,<br>5. Sensitization of employees regarding the handling of correction, deletion and restriction requests,<br>6. Notification pursuant to Art. 19 GDPR to all recipients to whom personal data have been disclosed of any rectification or erasure of personal data or restriction of processing pursuant to Art. 16 GDPR, Art. 17 para. 1 GDPR and Art. 18 GDPR, unless this proves impossible or involves disproportionate effort, |

| | |
|---|---|
| | 7. Consideration of any publications of the data,<br>8. correct consideration of the specifications and exceptions to cancellation in accordance with Art. 17 para. 1 and 3 GDPR,<br>9. Secure technical implementation taking into account<br>  ○ the irreversibility of deletions,<br>  ○ Inclusion of backups in the processes,<br>10. Informing the data subject about recipients to whom personal data has been disclosed if the data subject so requests.<br>• Sample documents are available for responding to data subject requests<br>• The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the data controller must provide evidence of the manifestly unfounded or excessive character of the request.<br>• If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>  ○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>  ○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• The controller informs the data subject of the measures taken without undue delay and in any case within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, he informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.<br>• The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>• Every request and its processing is documented by the controller. |

| | |
|---|---|
| | If the obligations under Art. 16, 17, 18 GDPR are not fulfilled by the controller in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. 16, 17, 18 GDPR.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in the processing of **requests for rectification, erasure, and restriction.** The corresponding instructions must be documented. In this context, the processor forwards any requests for rectification, erasure and restriction to the Controller and informs the data subject accordingly.<br>If the controller is unable to erase, rectify, or restrict the processing itself, the processor shall designate a contact person who can carry out the implementation, cf. the requirements in DP06.12, DP06.13. As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 17

| | |
|---|---|
| DP06.12 | **A) Controller**<br>The Controller must erase personal data at the request of the data subject. A deletion concept, e.g. in accordance with DIN 66398-2016, is documented, which specifies in particular:<br>▪ Scope of the deletion concept (e.g. which IT systems and databases)<br>▪ Definition of deletion periods<br>▪ Definition and concrete description of deletion mechanisms (documentation of the individual processes and implementation specifications)<br>  ○ When defining the minimum requirements for deletion procedures, the specifications of the BSI IT-Grundschutz-Compendium CON.6 Deletion and destruction must be met<br>▪ Definition of responsibilities and reporting channels with regard to the execution of deletions<br>▪ If a processor is used by the controller: Explanation o which deletion obligations are to be fulfilled by the processor<br>▪ Responsibilities with regard to monitoring the deletion processes<br>▪ Verification of the actual implementation and validity of the deletion<br>▪ Definition of how deletions are documented<br>▪ Inclusion of data deletion in backups and archives<br>▪ Regular evaluation (at least annually) of the selected deletion mechanisms to determine whether they still correspond to the state of the art<br>It must be ensured that deletions can be carried out without compromising the integrity of the remaining data.<br>An exception to the erasure obligation exists for the controller if the processing is necessary for one of the reasons set out in Art. 17 para. 3 |

| | |
|---|---|
| | GDPR. In the event of an exception to the erasure obligation, the Controller must state the reasons presented in Art. 17 para. 3 GDPR for not erasing personal data.<br>If data subjects are able to delete their data themselves, the Controller will provide a corresponding information.<br><br>• The controller informs the data subject of the measures taken without undue delay and in any case within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, he informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.<br>• The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the data controller must provide evidence of the manifestly unfounded or excessive character of the request.<br>• If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>  ○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>  ○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>• Every request and its processing is documented by the controller.<br>If the obligations under Art. 17 GDPR are not fulfilled by the controller in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. |

| | |
|---|---|
| | 17 GDPR.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as part of its obligation to follow instructions in the deletion of stored PD. The corresponding instructions must be documented. The Processor forwards any requests for erasure to the Controller and inform the data subject thereof. In addition, the obligation to provide support can also be fulfilled by enabling the controller to erase the data directly through technical measures. If the controller is unable to erase the data itself, the processor shall designate a contact person for the controller who can implement the erasure. Appropriate processes shall be established for this purpose, which shall specify in particular: Responsibilities and reporting channels with regard to the performance of deletions, deletion mechanisms including documentation of the individual processes or implementation specifications (when specifying the minimum requirements for deletion procedures, the specifications of BSI IT-Grundschutz-Compendium CON.6 Deletion and Destruction shall be implemented), responsibilities regarding the monitoring of deletion processes, verification of the actual implementation or effectiveness of the deletion, determination of how the implementation of deletion measures is documented, consideration of data deletion in backups and archives, regular evaluation (at least annually) of whether the selected deletion mechanisms still correspond to the state of the art.<br>As part of the support function, the Processor designates a contact person for the Controller.<br>If data subjects are able to delete their data themselves, the Processor must support the Controller in preparing a corresponding description, which must be provided to the data subject.<br>If the obligations under Art. 17 GDPR are not fulfilled by the processor in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. 17 GDPR. |

[GDPR] Art. 18

| | |
|---|---|
| **DP06.13** | **A) Controller**<br>The Controller must restrict the processing of personal data at the request of the data subject. The Controller verifies whether one of the following conditions is fulfilled:<br>a. the data subject contradicts the accuracy of the PD processed by the Controller<br>b. the data subject requests the restriction of processing instead of erasure due to unlawful processing<br>c. the data subject needs the PD for the establishment, exercise or defence of legal claims<br>The restriction is realized by<br>1. note of the reasons for the restriction of processing (see Art. 18 para. |

| | |
|---|---|
| | 1),<br>2. labelling of data records,<br>3. different processing options for correspondingly labelled data records in the IPS,<br>4. logging of the labelling carried out.<br>• The controller informs the data subject of the measures taken without undue delay and in any case within one month of receipt of the data subject's request. With regard to a possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR, if this is necessary taking into account the complexity and number of requests, it is ensured that the data subject is informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, he informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented.<br>• The information is provided free of charge. Only in the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or implementing the requested measure, or b) refuse to act on the request. In these cases, the data controller must provide evidence of the manifestly unfounded or excessive character of the request.<br>• If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>○ If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>○ The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>• The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>11. Every request and its processing is documented by the controller.<br>If the obligations under Art. 18 GDPR are not fulfilled by the controller in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. |

| | |
|---|---|
| | 18 GDPR.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as part of its obligation to follow instructions in restricting the processing of the PD.<br>The Processor describes within the documentation of the evaluation object how the processing of PD can be restricted.<br>The Processor forwards any requests to restrict the processing of PD to the Controller and inform the data subject thereof.<br>In addition, the obligation to provide support can also be fulfilled by enabling the controller to restrict the processing of the data through technical measures. If the controller is not able to restrict the processing itself, the processor shall designate a contact person for the controller who can restrict the processing. As part of the support function, the Processor designates a contact person for the Controller.<br>. |

[GDPR] Art. 20

| | |
|---|---|
| **DP06.14** | **A) Controller**<br>The data subject have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in **a structured, commonly used and machine-readable format** and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent pursuant to Art. 6 para. 1 or Art. 9 para. 2 GDPR or on a contract pursuant to Article 6 para. 1 lit. b GDPR and the processing is carried out by automated means.<br>For this purpose, the controller has implemented processes that regulate at least:<br>1. defined responsibilities including deadlines and communication channels with regard to the processing of requests for data portability<br>2. absence and substitution rules have been established to ensure compliance with existing deadlines<br>3. sensitization of employees regarding the handling of requests regarding data portability<br>4. when implementing the right to data portability, the controller must check the following requirements - the check steps must be documented:<br>a) The data subject must have provided their personal data to the controller. The following categories of data can be considered as “provided by the data subject”:<br>○ Data actively and voluntarily provided by the data subject<br>○ Observed data provided by the data subject through the use of the IPS<br>b) The personal data provided to the controller must relate to the data subject themselves<br>c) Processing by the controller is based on consent pursuant to Art. 6 para. 1 lit. a GDPR or Art. 9 para. 2 lit. a GDPR or on a contract |

| | |
|---|---|
| | pursuant to Art. 6 para. 1 lit. b GDPR<br>d) The processing of personal data is carried out using automated procedures<br>e) The processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller<br>5. Verification of the identity of the requesting person (authentication), see the requirements in **DP06.03**<br>6. The process takes into account the following deadlines: The controller provides the PD to the data subject without undue delay and in any case within one month of receipt of the data subject's request. A possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR is also taken into account in the process if this is necessary, taking into account the complexity and number of requests. The data subject will be informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, it informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented<br>7. The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>8. Every request and its processing is documented by the controller.<br>9. it must be ensured that the exercise of rights by data subjects does not adversely affect the rights and freedoms of other persons<br>10. if no PD are processed by the controller and therefore no data can be transferred, the data subject is informed of this.<br>11. The data transfer is free of charge. Only in the case of manifestly unfounded or - in particular in the case of frequent repetition - excessive requests by a data subject, the controller may either a) demand a reasonable fee, taking into account the administrative costs of providing the information or notification or carrying out the requested action, or b) refuse to act on the request. In these cases, the controller must provide evidence of the manifestly unfounded or excessive character of the request<br>12. It is ensured that the data subject receives the PD concerning him/her in a structured (presentation of the data in a structured manner), common (format is generally used) and machine-readable format (if it is "in a file format that is structured in such a way that software applications can easily identify, recognize and extract the specific data. Both digital and paper-based, scannable formats that enable software or computer-controlled processing are recorded). When determining the format in which the PBD is provided, it is necessary to focus on the industry- and region-specific context, with XML, JSON and CSV formats being particularly preferable. The selected format must be documented. |

| | |
|---|---|
| | 13. The direct transfer to another Controller is supported as far as technically possible (Art. 20 para. 2 GDPR).<br>If the obligations under Art. 20 GDPR are not fulfilled by the controller in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. 20 GDPR.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in the transfer of the PD in a structured, common, and **machine-readable format.** The Processor forwards any requests to provide PD in a structured, common, and machine-readable format to the Controller and inform the data subject thereof.<br>In addition, the obligation to provide support can be fulfilled by the processor making it technically possible to extract and transmit the personal data in a structured, commonly used, and machine-readable format, e.g., by implementing an export function in XML, CSV, or JSON format.<br>As part of the support function, the Processor designates a contact person for the Controller and provide the Controller with all information to enable the Controller to implement the right to data portability. |

[GDPR] Art. 21 para. 1

| | |
|---|---|
| DP06.15 | **A) Controller**<br>The Controller must realize the request of a data subject to exercise their right to object to the processing of PD. In context of the implementation of the right to object the Controller regards the following:<br>a) Right to object according to Art. 6 Abs. 1 UAbs. 1 lit. e or f (Art. 21 Abs. 1 GDPR)<br>1. Provision of appropriate communication channels or provision of technical functions that ensure that an objection can be made at any time.<br>2. The Controller must ensure that data subjects, can effectively assert their rights on all communication channels used against them.<br>3. informing the data subjects about the existence of the right to object, cf. the requirements in DP06.16.<br>4. Definition of personnel responsibilities regarding the handling of objections to the processing of personal data<br>5. Sensitizing employees regarding the right of objection<br>6. Absence and substitution rules are in place to ensure that existing deadlines are met.<br>7. The objection must be based on grounds relating to the particular situation of the data subject.<br>• The data subject must provide reasons that arise from their particular situation. The data subject will be notified accordingly. |

| | |
|---|---|
| | 8. Verification of the validity of the objection and the existence of any exceptions to the right of objection. If the controller has legitimate grounds for refusing to comply with the objection, it carries out a balancing of interests, demonstrating its legitimate grounds for processing which override the interests, rights, and freedoms of the data subject, or assert that the processing is necessary for the establishment, exercise, or defense of legal claims. Sample documents for carrying out the balancing of interests are available.<br>9. The process takes the following deadlines into account: The controller decides and informs the data subject without delay of the measures taken without undue delay and in any case within one month of receipt of the data subject's request. A possible extension of the deadline by a further two months in accordance with Art. 12 para. 3 sentences 2 and 3 GDPR is also taken into account in the process if this is necessary, taking into account the complexity and number of requests. The data subject will be informed of an extension of the deadline within one month of receipt of the request, together with the reasons for the delay. Sample documents are available for this purpose. If the controller does not take action at the request of the data subject, it informs the data subject without delay, but at the latest within one month of receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy, in accordance with Art. 12 para 4 GDPR. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented<br>10. The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>11. Every request and its processing is documented by the controller.<br>12. Determination of how communication with the data subject will take place: If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>• If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>• The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>13. If the data subject has objected to the processing and it has not yet been determined whether the legitimate reasons of the controller outweigh those of the data subject, the processing is restricted in accordance with Art. 18 para. 1 lit. d GDPR, cf. **DP06.11**.<br>14. If there is no reason for further processing and the objection was effective, the controller must terminate the processing measures immediately, taking into account the scope, the PD must be deleted (cf. Art. 17 para. 1 lit. c Var. 1 GDPR). For this technical functions to terminate the processing associated with the objection and with regard to the |

| | |
|---|---|
| | deletion of the PD, cf. the requirements in **DP06.11** are in place.<br>15. If the controller has made the personal data public, it informs third parties who process the data about the request for erasure (Art. 17 (2) GDPR). (Art. 17 para. 2 GDPR). Appropriate processes (responsibilities, communication channels) are in place for this, see the requirements in **DP06.11**.<br>16. The right to object is exercised free of charge. Only in the case of manifestly unfounded or excessive requests from a data subject, particularly where they are repetitive, may the controller either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or b) refuse to act on the request. In such cases, the controller must provide evidence of the manifestly unfounded or excessive nature of the request.<br><br>b) <u>Right to object to the use of data for direct marketing (Art. 21 para. 2 and para. 3 GDPR)</u><br>If the data subject objects to processing for **direct marketing purposes** (objection to advertising), including profiling, insofar as this is related to this direct marketing, it is ensured that the data is no longer processed for these purposes, Art. 21 para. 3 GDPR. Appropriate processes are in place for this, which at least provide for this:<br>1. Provision of appropriate communication channels or provision of technical functions that ensure that an advertising objection can be made at any time<br>2. Informing the data subjects about the existence of the right to object, cf. the requirements in **DP06.16**.<br>3. Definition of responsible persons with regard to the processing of advertising objections that ensure immediate processing<br>4. The process takes the following deadlines into account: The controller decides and inform the data subject of the measures taken without delay, but in any case within one month of receiving the request from the data subject. Similarly, any extension of the deadline by a further two months in accordance with Art. 12 (3) sentences 2 and 3 GDPR is taken into account in the process if this is necessary in view of the complexity and number of requests. The data subject is informed of any extension of the deadline, together with the reasons for the delay, within one month of receipt of the request. Sample documents are available for this purpose. If the controller does not act on the request of the data subject, it informs the data subject without delay, but no later than one month after receipt of the request, of the reasons for this and of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are also available for this purpose. Responsibilities for monitoring compliance with the deadlines are documented. A decision to refuse a request must be justified in accordance with Art. 12 (4) GDPR and the data subject is informed of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. Sample documents are available for this purpose.<br>5. The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain lan- |

| | |
|---|---|
| | guage; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>6. Every request and its processing is documented by the controller.<br>7. Determination of how communication with the data subject will take place: If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>• If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>• The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>8. Sample documents are available to inform the data subject, or technical implementation ensures this<br>9. Objection to advertising can be made without giving reasons. The data subject is not required to provide a reason.<br>10. The advertising objection can be made without additional hurdles or complications<br>11. Where possible, it must be possible to exercise the right to object immediately, e.g. by means of a checkbox or link, an objection option, settings in the customer portal.<br>12. Implementation of technical and organisational measures to ensure that PD is no longer used for direct marketing purposes<br>13. If the data subject objects to processing for direct marketing purposes, the personal data will no longer be processed for direct marketing purposes, including any profiling measures, and the data sets used for direct marketing purposes will be deleted immediately. Technical functions for terminating direct marketing and deleting the PBD are available for this purpose; see the requirements in **DP02.08, DP06.11, DP06.12**.<br>14. Inclusion of the PD in an advertising blocking file, which prohibits the use of data for direct marketing purposes in the future.<br>15. Guarantee that up-to-date databases are used at all times<br>16. If the PD is included in an advertising blocking file, the data subjects must be informed about the purpose of the inclusion of their data in a blocking file.<br>17. The right to object is exercised free of charge. Only in the case of manifestly unfounded or excessive requests from a data subject, particularly where they are repetitive, may the controller either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or b) refuse to act on the request. In such cases, the controller must provide evidence of the manifestly unfounded or excessive nature of the request.<br><br>c) Right to object to the use of data for scientific, historical or statistical purposes (Art. 21 para. 6 GDPR)<br>Data subjects may object to the processing of their personal data for scientific, historical, or statistical purposes within the meaning of Art. 89 para. |

| | |
|---|---|
| | 1 GDPR. The following conditions must be met:<br>1. Processing is carried out for scientific, historical, or statistical purposes in accordance with Art. 89 para. 1 GDPR<br>2. The objection must be based on grounds relating to the particular situation of the data subject. The data subject, must present reasons that arise from their particular situation and which have not yet been taken into account within the framework of Art. 6 para. 1 lit. e GDPR or Art. 89 para. 1 GDPR.<br>3. Controller must weigh up the conflicting interests and demonstrate that the processing is necessary for the performance of a task carried out in the public interest. Appropriate responsibilities have been defined and sample documents are available for carrying out the balancing of interests.<br>4. The Controller may object to the processing on the grounds that the processing is necessary for the performance of a task carried out in the public interest, cf. the requirements in **DP03.06**, or because there are other exceptions pursuant to Art. 89 para. 2 and 3 GDPR and Art. 23 GDPR<br>5. Existence of technical functions to terminate the processing associated with the objection and with regard to the deletion of the PD, cf. the requirements in **DP02.08**, **DP06.11, DP06.12**<br>6. The information to the data subject is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; this applies in particular to information aimed specifically at children, cf. the requirements in **DP06.01**<br>7. Confirmation of an effective objection to the data subject<br>8. Determination of how communication with the data subject will take place: If the data subject has submitted the request in electronic form, communication takes place electronically wherever possible, unless the data subject requests a different means of communication.<br>• If requested by the data subject, the information may be provided orally, provided that the identity of the data subject has been proven in another form. The controller must specify how such proof of identity can be provided.<br>• The controller documents: the desire for information in oral form, the procedure used to verify the identity of the data subject, if applicable, the fact that the information was provided to the data subject<br>9. Every request and its processing is documented by the controller.<br>10. The right to object is exercised free of charge. Only in the case of manifestly unfounded or excessive requests from a data subject, particularly where they are repetitive, may the controller either a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or b) refuse to act on the request. In such cases, the controller must provide evidence of the manifestly unfounded or excessive nature of the request.<br><br>If the obligations under Art. 21 GDPR are not fulfilled by the controller in accordance with Art. 23 GDPR due to a legal provision of the Union or Germany, it must be documented which legal basis from Union law or German law in conjunction with Art. 23 GDPR is used and to what extent there is a corresponding restriction of the rights and obligations under Art. |

| | |
|---|---|
| | 21 GDPR.<br>The specification of the individual requirements can be found in the evaluation notes.<br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in the processing of **objections to the processing** of PD.<br>The obligation to provide support is implemented in particular through:<br>1. Implementation of processes to ensure that objections to processing are forwarded to the controller. In this context, contact persons are named for the Controller, communication channels are defined and responsibilities for processing corresponding data subject inquiries are defined. The processor provides the controller with all information required to implement the right to withdraw consent.<br>2. The IPS documentation, which is made available to the controller, contains a reference to the fact that the controller is obliged to respond to objections by the data subject.<br>As part of the support function, the Processor designates a contact person for the Controller. |

[GDPR] Art. 21 para. 4

| | |
|---|---|
| DP06.16 | **A) Controller**<br>The Controller informs data subjects about the existence of a right to object to the processing of PD pursuant to Art. 21 para. 1 GDPR at the time of obtaining PD.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions in providing information on the **right to object** in accordance with Art. 21 para. 1 GDPR.<br>In this context, the Processor provides documentation on the IPS, which informs that the Controller is obliged to inform data subjects of the existence and exercise of their right to object.<br>As part of the support function, the Processor designates a contact person for the Controller |

[GDPR] Art. 22

| | |
|---|---|
| DP06.17 | **A) Controller**<br>The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.<br>1. This does not apply if the decision: |

a) is necessary for the conclusion or performance of a contract between the data subject and the Controller.
   - The automated decision must be objectively necessary for the conclusion or fulfilment of a contract with a data subject. Necessity must be interpreted narrowly.
   - The Controller must be able to demonstrate that the automated decision is necessary, in particular that contracts cannot be managed without the use of automated procedures.
   - The necessity must be documented.

b) is authorised by European Union or German law to which the Controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
   - There must be a legal obligation on the Controller and the obligation must relate directly to automated decisions.
   - The obligation is related to the data subject.
   - The legal obligation must arise from European Union law or German law to which the Controller is subject.
   - It must be documented which legal basis from European Union law or German law in conjunction with Art. 22 para. 2 lit. b GDPR is used.
   - The relevant legislation must contain appropriate measures to safeguard the rights and freedoms and the legitimate interests of the data subject (in particular specific information to the data subject, right to direct intervention by a person, presentation of the data subject's own position, explanation of the decision taken following an appropriate assessment, right to challenge the decision)

c) with the express consent of the data subject, see the requirements for consent in **DP04**.
   - Consent must be given in an informed manner. The data subject must be provided with information about the purpose of the automated decision-making process (cf. **DP06.04** and **DP06.05**). In addition, information about the logic involved and the scope and intended effects of automated decision-making for the data subject must be provided.
   - The declaration of consent must be given explicitly, i.e. it must explicitly refer to the fact that the decision in question is based exclusively on an automated decision.
   - Consent must be given voluntarily.
   - The declaration of consent must explicitly refer to consent to the automated decision.
   - Consent must be documented.
   - It must be possible to withdraw consent, cf. the requirements in **DP04.06, DP04.07, DP04.08**

With regard to the requirements for consent, the EDPB's Guidelines 05/2020 on Consent under Regulation 2016/679, version 1.1, adopted on 4 May 2020, must be taken into account when applying this criterion.

2. The Controller must implement the data protection principles in accordance with Art. 5 GDPR for all profiling activities and automated decisions, see the respective requirements in **DP02**.

| | |
|---|---|
| | 3. The Controller must inform the data subjects about the existence of automated decision-making including profiling in accordance with Art. 22 para. 1 and 4 GDPR and - at least in these cases - provide meaningful information about the logic involved and the scope and intended effects of such processing for the data subject (Art. 13 para. 2 lit. f GDPR, Art. 14 para. 2 lit. g GDPR), cf. the requirements in **DP06.04** and **DP06.05**. It must be explained clearly and simply to the data subjects how profiling or automated decisions work.<br>4. Data subjects must be informed of their rights under Art. 22 para. 3 GDPR, where relevant.<br>5. The data subject has the right to obtain information on the personal data used for profiling purposes, including the categories of data used for profiling, cf. the requirements in **DP06.07**. In addition, the input data used for profiling must be made available and information on the profile and details of the segments into which the data subject has been categorised must be provided, Art. 15 para. 3 GDPR.<br>6. Processes regarding correction, deletion, and restriction requests with regard to profiling must be implemented, cf. the requirements in **DP06.11.**<br>7. Appropriate mathematical or statistical procedures are used and technical and organisational measures are implemented to ensure, in particular, that factors leading to inaccurate personal data are corrected and the risk of errors is minimised, and to secure personal data in such a way take into account potential threats to the interests and rights of the data subject, and prevent, inter alia, discriminatory effects or processing that has such an effect on natural persons based on race, ethnic origin, political opinion, religion or belief, trade union membership, genetic predisposition or health status and sexual orientation, cf. Recital 71 GDPR.<br>8. The minimum requirements pursuant to Art. 22 para. 3 GDPR are met: The data subject must have the opportunity to present their point of view to the Controller, to have the decision reviewed by a natural person and to contest the decision made. The Controller must therefore have implemented processes that ensure that a decision made by automated means is reviewed by a natural person on the part of the Controller in an open-ended manner and on the basis of the specific individual facts of the case, if the data subject requests this. The point of view of the data subject must be taken into account. In particular, the implemented processes must make provisions for: detailed information for the data subjects about the logic involved and the scope and intended effects of such processing and their rights in accordance with Art. 22 para. 3 GDPR, communication channels for the data subject, determination of Controller, persons responsible for dealing with the facts of the case by a natural person (where appropriate taking into account the point of view of the data subject, documentation of the review, on request, the data subject must be informed of the main reasons for the rejection of their request, manner of explaining the decision taken after the assessment, offer of measures to enable the data subject to take corrective action).<br>9. As a rule, children are not affected by exclusively automated decision-making. Only in exceptional cases is the processing of children's data carried out on the basis of the exceptions in Art. 22 para. 2 lit. a, b, c |

| | |
|---|---|
| | GDPR. In this case, appropriate safeguards must be in place (see requirements above) to ensure that the rights, freedoms and legitimate interests of the children whose data are processed are effectively protected by these safeguards.<br>10. Pursuant to Art. 22 para. 4 GDPR, an automated decision involving special categories of personal data is only permissible if the following cumulative conditions are met and if the Controller has taken appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject.<br>a) An exception applies in accordance with Art. 22 para. 2 GDPR, see above<br>b) Art. 9 para. 2 lit. a GDPR (explicit consent of the data subject to the processing of special categories of personal data) applies, cf. the requirements in **DP05.01**<br>c) or Art. 9 para. 2 lit. g GDPR applies (processing is necessary on the basis of European Union or German law for reasons of substantial public interest), cf. the requirements in **DP05.01**<br>▪ Appropriate measures have been taken to protect the rights and freedoms as well as the legitimate interests of the data subject (minimum requirements pursuant to Art. 22 para. 3 GDPR (cf. the requirements in **DP08**), fulfilment of the information to be provided (cf. the requirements in **DP03**), transparency of the logic involved, use of appropriate mathematical or statistical procedures (cf. the requirements in **DP07**).<br>11. A data protection impact assessment has been carried out, see the requirements in **DP10.**<br>The guidelines on automated individual decision-making, including profiling, for the purposes of Regulation 2016/679, adopted on 3 October 2017 (WP251rev.01), endorsed by the EDPB, last revised and adopted on 6 February 2018, of the Article 29 Working Party, endorsed by the EDPB, must be taken into account when applying this criterion.<br>The specification of the individual requirements can be found in the evaluation notes.<br><br>**B) Processor**<br>The Processor supports the Controller in accordance with Art. 28 para. 3 sentence 2 lit. e GDPR as far as possible and as part of its obligation to follow instructions with regard to responding to requests from data subjects, concerned persons in connection with Art. 22 GDPR.<br>In this context, the Processor provides the Controller with documentation of the IPS, which informs that the Controller is obliged to inform the data subject of the existence of the right not to be subject to a decision based solely on automated processing, including profiling. As part of the support function, the Processor designates a contact person for the Controller. |

## DP07 Controller and Processor

[GDPR] Art. 24 para. 1, 2

| | |
|---|---|
| DP07.01 | **A) Controller**<br>The processes associated with the IPS contain **specifications for suitable technical and organisational measures** that ensure compliance with data protection requirements.<br>In particular, regarding the requirements in DP07.02, it must be ensured:<br>• Carrying out a risk analysis, see the requirements for this in DP02.07 and DP07.02<br>• Maintaining the record of processing activities, cf. the requirements in DP07.11<br>• Appointment of a data protection officer, see DP09.03<br>• Implementation of processes regarding the safeguarding of data subject rights, see DP06<br>• Implementation of processes for dealing with personal data breaches, see the requirements in DP09.01 and DP09.02<br>• Definition of fixed contact persons in the organisational units of a company for the data protection officer and the employees of the respective organisational units in matters of data protection<br>• Existence of substitution arrangements for absent employees<br>• If, within the evaluation object, there is a possibility that data subjects may make their PBD visible to other users or third parties, e.g., information from social media profiles, comments posted, the controller ensures that visibility is not the default setting and that the PBD is not made accessible to an indefinite number of natural persons without the data subject's intervention. Instead, data subjects can determine the scope of visibility of their PBD and the content they share themselves. A function is implemented that enables the data subject to view their stored PD.<br>• A function has been implemented to ensure that a copy of the PD is made available to the person.<br>• A data portability function has been implemented.<br>• Implementation of data protection training for employees, cf. the requirements in DP09.08<br>• Obligation of employees to maintain confidentiality and data protection<br>• Encryption of data carriers, see also the requirements in DP08<br>• Existence of password guidelines, see also the requirements in DP08<br>• Logging of accesses, see also the requirements in DP08<br>• Establishment and control of authorisations, see also the requirements in DP08<br>• Implementation of automatic blocking and deletion routines, pseudonymisation and anonymisation procedures<br>• Technical measures, e.g. hashing and encryption, are used to limit the possibility of personal data being used for a new purpose and organisational measures are used to limit the reuse of personal data, e.g. contractual obligations.<br>• Regular checks are carried out to ensure that the processing is |

| | |
|---|---|
| | necessary for the purposes for which the data was collected and that the processing is carried out in compliance with the purpose limitation aspect.<br>• Technical options are provided for minimising the processed PD depending on the respective processing situation.<br>• Personal data is pseudonymised as soon as there is no longer a need for directly identifiable personal data and the identification keys must be stored separately.<br>• Personal data is anonymised or deleted if it is not or no longer necessary for the purpose.<br>• Where possible, aggregated data is used.<br>• Definition of a rights-roles concept according to the principle of necessity<br>• Procedures and functions for the deletion and/or anonymisation of PD are implemented, cf. the requirements in **DP02.08**<br>• An erasure concept is in place, see the requirements in **DP02.08**<br>• An access and authorisation concept ensures that as few people as possible have access to the PD to perform their tasks.<br>• If pseudonymisation techniques are used, the specific implementation is described.<br>• If anonymisation techniques are used, the specific implementation is described.<br>• The structure of the data or database must be designed in such a way that individual data fields, data records or groups of data can be corrected, e.g. by the data subject themselves.<br>• All correction and deletion processes must be documented.<br>• Technical and organisational measures are implemented to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage, see also the requirements in DP08.<br>• The effectiveness of the implementation of the safety requirements is regularly reviewed. Corresponding responsibilities and the manner of the review are defined for this purpose.<br>• Data transmissions are protected against unauthorised and unintentional access and against unauthorised and unintentional changes, see also the requirements in DP08.<br>• Data storage is protected against unauthorised access and unauthorised changes, see also the requirements in **DP08**.<br>• Backups and log files are protected against unauthorised and unintentional access and against unauthorised and unintentional changes, see also the requirements in **DP08**. |

[GDPR] Art. 25 para. 1 in conjunction with Art. 5 para. 1

| | |
|---|---|
| **DP07.02** | **Controller**<br>The Controller must take appropriate technical and organisational measures for the effective implementation of the data protection principles pursuant to Art. 5 para. 1 GDPR and integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of the data subjects. In this context, the Controller must take into account the state of the art, the costs of implementation and the |

| | |
|---|---|
| | nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.<br>The Controller must take into account the EDPB's Guidelines 4/2019 on Article 25 Data protection by design and by default, version 2.0, adopted on 20 October 2020, when regarding the implementation of appropriate measures in connection with data protection by design In particular, the Controller must ensure:<br>1. Data protection aspects must already be taken into account in the initial planning phase of a processing operation, even before the means of processing are determined. Appropriate processes and work instructions, e.g. data protection guidelines for IT developers, must be implemented for this purpose.<br>2. The Controller must ensure that the Data Protection Officer is involved in the procurement and development procedures and throughout the entire processing cycle. Appropriate processes must be implemented for this purpose (definition of responsibilities, definition of how and when the Data Protection Officer is to be involved, definition of what information is to be made available to the Data Protection Officer).<br>3. Measures that ensure compliance with data protection in the company, e.g. when changes are made to data protection law or IT procedures, e.g. carrying out ad hoc checks, processes relating to the early involvement of the data protection officer (definition of how and when the data protection officer is to be involved, participation of the data protection officer in management meetings, regular meetings of the data protection officer with IT officers and information security officers).<br>4. Compliance with the principle of data protection by design must be taken into account throughout the entire processing life cycle.<br>5. The Controller documents the implemented technical and organisational measures. In addition to the specific measures, the decision-making process, including the aspects and reasons why certain measures were or were not implemented, must also be documented.<br>6. When selecting the technical and organisational measures, the Controller must take the following aspects into account: the state of the art, the implementation costs, the type, scope, circumstances and purpose of the processing as well as the different probability of occurrence and severity of the risks associated with the processing for the rights and freedoms of natural persons.<br>7. The Controller must establish performance indicators in order to prove the effectiveness of the measures implemented.<br>8. The data protection principles pursuant to Art. 5 GDPR and Recital 39 GDPR when processing personal data must be implemented by means of data protection through technology design. Controllers must examine how compliance with the data protection principles can be ensured for each specific processing operation.<br>a) Transparency, cf. the requirements in **DP02.01**<br>b) Lawfulness, cf. the requirements in **DP02.03**<br>c) Fairness and transparency processing, cf. the requirements in **DP02.02**<br>d) Purpose limitation, cf. the requirements in **DP02.04**<br>e) Data minimisation, cf. the requirements in **DP02.06**<br>f) Accuracy, see the requirements in **DP02.07, DP06.11** |

| | |
|---|---|
| | g) Memory limitation, see the requirements in **DP02.08**<br>h) Integrity and confidentiality, cf. the requirements in **DP02.09, DP08**<br>i) Accountability, cf. the requirements in **DP02.10**<br>9. The implementation of the data protection principles and the rights of the data subjects is described (accountability), cf. the requirements in **DP02.10,** and implementation within the organisation is required, e.g. internal policy or data protection concept.<br>The specification of the individual requirements can be found in the test notes. |

[GDPR] Art. 25 para. 2

| | |
|---|---|
| **DP07.03** | **Controller**<br>The IPS supports the Controller by taking appropriate (cf. the following requirements – No.1 to 8) technical and organisational measures to ensure that personal data is only processed to the extent necessary for the respective purpose by means of standard default settings.<br>This applies to:<br>• Quantity of PD collected<br>• Scope of the processing of PD,<br>• Storage period of the processed PD,<br>• Access to PD<br>With regard to the implementation of the **principle of "Privacy by default - data protection-friendly default settings"**, the EDPB's Guidelines 4/2019 on Article 25 Data protection by design and by default, version 2.0, adopted on 20 October 2020, must be taken into account. In particular, it must be ensured that:<br>1. Data protection-friendly default settings must already be taken into account in the initial phase of planning a processing operation, even before the means of processing are determined. Appropriate processes and work instructions, e.g. data protection guidelines for IT developers, must be implemented for this purpose.<br>2. The Data Protection Officer must be involved in the procurement and development procedures and throughout the entire processing cycle. Appropriate processes must be implemented for this purpose (definition of responsibilities, definition of how and when the data protection officer is to be involved, definition of what information is to be made available to the data protection officer).<br>3. Compliance with the principle of data protection by default must be taken into account throughout the entire processing life cycle.<br>4. Purposes of the processing must be clearly defined and documented.<br>5. The technical and organisational measures implemented must be documented.<br>6. The implementation of data protection through data protection-friendly default settings is described and implementation within the organisation is required, e.g. internal policy or data protection concept.<br>7. Data protection-friendly default settings limit the collection, processing and disclosure of personal data to the minimum required for the intended purpose (necessity). Purposes of the processing must be clearly defined and the necessity of the processing must be documented. Key aspects of data protection through data protection- |

| | |
|---|---|
| | friendly default settings are listed below. However, this list is not exhaustive and is merely exemplary.<br>a) Quantity and scope of processing<br>■ Only personal data that is appropriate, relevant and limited to what is necessary for the purpose is processed.<br>■ Technical options are provided for minimising the processed PD depending on the respective processing situation.<br>■ Personal data is pseudonymised as soon as there is no longer a need for directly identifiable personal data and the identification keys must be stored separately.<br>■ Free text fields are used sparingly and each free text field must be provided with a purpose description.<br>■ Mandatory fields are used sparingly and are clearly labelled.<br>■ An access and authorisation concept ensures that as few people as possible have access to the PD to perform their tasks.<br>■ If optionality is given with regard to the collection and processing of personal data, each option is deactivated by default.<br>■ For the collection and processing of personal data, each option is disabled by default, and<br>■ These settings must only be activated by explicit choice of the data subject.<br>■ Certain functions are deactivated or restricted by default, e.g. camera and microphone functions<br>■ Assistance systems are deactivated or restricted by default.<br>■ Autostart functions are deactivated or restricted.<br>■ The automatic connection to networks or the Internet is deactivated or restricted by default.<br>■ User interfaces, e.g. in terms of size, shape, colour of buttons, are designed in such a way that the perception and decisions of the data subjects are not biased in a certain direction, so-called dark patterns.<br>■ Default settings are implemented that minimise and restrict the linking options.<br>■ Depersonalisation or other data minimisation techniques are used.<br>■ If pseudonymisation techniques are used, the specific implementation is described.<br>■ If anonymisation techniques are used, the specific implementation is described.<br>■ The mechanisms, e.g. technical system configurations, that are implemented to ensure data minimisation are documented.<br>b) Storage period of the processed PD<br>■ Storage periods are kept as short as possible by default settings.<br>■ A deletion concept has been implemented to ensure that personal data is automatically deleted after the storage period has expired.<br>■ Personal data is anonymised or deleted if it is not or no longer necessary for the purpose.<br>■ Where possible, aggregated data is used.<br>■ Procedures and functions for the deletion and/or anonymisation of PD are implemented.<br>■ An extinguishing concept is in place. |

| | |
|---|---|
| | ▪ It is ensured that anonymised data cannot be re-identified and deleted data cannot be restored and appropriate tests are carried out.<br>▪ The deletion of certain PD is automated.<br>▪ The respective storage period, where possible including the corresponding legal basis, is documented.<br>▪ The deletion concept takes backups and log files into account.<br>▪ Processes have been implemented to check the execution and effectiveness of deletions (responsibilities for reviewing the execution of deletions, including determining the manner and frequency of review).<br>c) Accessibility of the PD<br>▪ A role and authorisation concept has been implemented to ensure that access is based on the need-to-know principle.<br>▪ An authorisation concept has been implemented to ensure that access to particularly sensitive data only takes place in compliance with the dual control principle.<br>▪ Set up a preset strong access protection, e.g. password defaults<br>▪ Technical and organisational measures are implemented to protect the PD from unauthorised or unlawful processing, see also the requirements in **DP08**<br>▪ Data transmissions are protected against unauthorised and unintentional access and against unauthorised and unintentional changes.<br>▪ Data storage is protected against unauthorised access and unauthorised changes.<br>▪ The strength of selected passwords is measured and displayed to support secure password assignment.<br>d) Making PD available to an indefinite number of persons<br>▪ If PD is to be made accessible to an undefined number of natural persons, the data subject, must consciously configure or intervene. Appropriate intervention options must be implemented, e.g. obtaining consent to the provision of PD to an undefined number of persons, existence of corresponding privacy settings by default.<br>8. The implementation of the principle of "privacy by default - data protection-friendly default settings" is described (accountability), cf. the requirements in **DP02.10,** and implementation within the organisation is required, e.g. internal policy or data protection concept.<br>The specification of the individual requirements can be found in the test notes. |

[GDPR] Art. 28 GDPR

| | |
|---|---|
| **DP07.04** | **A) Controller**<br>All Processors used, including sub-processors, are documented.<br>It must be demonstrated that these are indeed processors. The extent to which each entity actually has influence on the purposes and means of processing must be assessed as part of a case-by-case analysis. An examination of the specific data records or processes must be carried out |

| | |
|---|---|
| | and documented accordingly for classification as a Controller or Processor.<br>In particular, it must be demonstrated that the following requirements are met with regard to the existence of a Processor.<br>1. The Processor is a separate entity from the Controller, i.e. the processing activity is delegated in whole or in part to an external organisation.<br>2. Data processing is carried out on behalf of the Controller.<br>3. Personal data is only processed on the instructions of the Controller, and accordingly it is ensured that the Processor does not decide on the purpose and essential means of data processing. With regard to the assessment of the materiality of the means, the EDPB's standard applies in accordance with Guidelines 07/2020 on the terms "Controller" and "Processor" in the GDPR, version 2.0, adopted on 7 July 2021 (see evaluation note).<br>4. The Processor may not carry out processing for its own purposes.<br>The Controller must also explain whether there are sector-specific regulations for the area of application of the IPS that provide for special conditions for Processor or exclude them altogether.<br>The specification of the individual requirements can be found in the evaluation notes.<br><br>**B) Processor**<br>All Processors including sub-processors used are documented. In this context, it must be demonstrated that they are in fact contract processors.<br>The extent to which each entity actually has influence on the purposes and means of processing must be assessed as part of a case-by-case analysis. An examination of the specific data records or processes must be carried out and documented accordingly for classification as a Controller or Processor.<br>In particular, it must be demonstrated that the following requirements are met with regard to the existence of a Processor.<br>1. The Processor is a separate entity from the Controller, i.e. the processing activity is delegated in whole or in part to an external organisation.<br>2. Data processing is carried out on behalf of the Controller.<br>3. Personal data is only processed on the instructions of the Controller, and accordingly it is ensured that the Processor/sub-processor does not decide on the purpose and essential means of data processing. With regard to the assessment of the materiality of the means, the standard according to guidelines 07/2020 on the terms "Controller" and "Processor" in the GDPR, version 2.0, adopted on 7 July 2021, applies (see evaluation note).<br>4. The Processor may not carry out processing for its own purposes.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 28 para. 1

| | |
|---|---|
| DP07.05 | **Controller**<br>The Controller only works with Processors, who offer **sufficient guarantees that** appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR - also with regard to the security of the processing - and ensures the protection of the rights of the data subjects.<br>When assessing whether the Processor's guarantees are sufficient, the Controller must take the following elements into account:<br>a) Suitability of the technical and organisational measures offered<br>b) Expertise of the Processor<br>c) Reliability of the Processor<br>d) Resources of the Processor<br>The Data Protection Officer must be involved in the selection process at an early stage.<br>The Controller must ensure on an ongoing basis during the contractual relationship that sufficient guarantees are provided by the Processor. Processes for monitoring processors must be implemented and documented. Responsibilities, the type and manner of the monitoring (e.g. submission of certificates, reports from an independent auditor, current security concept, information from the processor, e.g. in a questionnaire, on-site inspection, reports from certified public accountant, internal revision or data protection officer) and monitoring intervals (depending on the risk associated with the processing, usually annually; if this interval is deviated from, this must be documented and justified) must be defined. The performance of the monitoring must be documented.<br>The specification of the individual requirements can be found in the test notes. |

[GDPR] Art. 28 para. 2

| | |
|---|---|
| DP07.06 | **Controller and Processor**<br>1. If the processor intends to commission further processors (sub-processors), it must obtain written, separate or general authorisation from the controller.<br>The Controller and Processor must define the procedure for authorising the use of sub-processors.<br>2. the role of the individual sub-processors is clearly recognisable on the basis of the agreements and descriptions assigned to the IPS. An overview of the authorised sub-processors is included in the agreement between Controller and Processor (Data Processing Agreement) or an annex thereto and must always be kept up to date.<br>3. in the case of general authorisation, the Processor must always inform the Controller of any intended change with regard to the involvement or replacement of other sub-processors. This must give the Controller the opportunity to object to such changes.<br>The specification of the individual requirements can be found in the test notes. |

[GDPR] Art. 28 para. 4

| | |
|---|---|
| DP07.07 | **Processor**<br>1. The Processor must impose on all **sub-processors,** by means of a contract or other legal instrument under European Union law or German law concerned, **the same data protection obligations** to which the Processor has committed itself towards the Controller.<br>**2.** The Processor only works with **sub-processors** that provide **sufficient guarantees that** appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR - also with regard to the security of the processing - and ensures the protection of the rights of the data subjects.<br>When assessing whether the guarantees provided by the sub-processor are sufficient, the Controller must take the following elements into account:<br>a) Suitability of the technical and organisational measures offered<br>b) Expertise of the sub-processor<br>c) Reliability of the sub-processor<br>d) Resources of the sub-processor<br>The Data Protection Officer must be involved in the selection process at an early stage.<br>The Processor must ensure on an ongoing basis during the contractual relationship that sufficient guarantees are provided by the sub-processor.<br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. 28 para. 4

| | |
|---|---|
| DP07.08 | **Sub-processor**<br>Where a processor engages another processor (sub-processor) pursuant to Article 28 para. 4 GDPR for carrying out specific processing activities on behalf of the controller, the following requirements must be fulfilled:<br>1. The controller must have given written, separate or general authorization to use the sub-proessor, see DP07.06.<br>2. This sub-processor must be subject to the same data protection obligations imposed by contract or other legal instrument under Union or German law as those laid down in the contract or other legal instrument between the controller and the processor according to Art. 28 para. 3 GDPR (see DP07.09) (including providing sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject).<br>Imposing the “same” obligations should be construed in a functional rather than in a formal way: that means it must be ensured that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included “by default” in the contract with the sub-processor (e.g., notification of a personal data breach by a sub-processor directly to the controller, forwarding of data subject requests directly to the controller). In this context, specifications must be made as to how the support obligations pursuant to Art. 28 (3) (e) and (f) GDPR should be fulfilled by the sub-processor.<br>In this regard, agreements must be made between the processor and the sub-processor as to whether, in the event of data subject requests, the sub-processor should first notify the processor, who will then inform the controller, or whether the sub-processor should notify the controller directly of the data subject request.<br>In addition, agreements must be made between the processor and the sub-processor as to whether, in the event of a personal data breach, the sub-processor should first notify the processor, who will then inform the controller, or whether the sub-processor should notify the controller directly.<br>If the notification of a personal data breach or the forwarding of a data subject request should be made directly by the sub-processor to the controller, the sub-processor must have processes in place to ensure that the controller is notified (definition of responsibilities and communication channels, determination of what information is communicated to the controller).<br>If the notification of a personal data breach or the forwarding of a data subject request should be made directly by the sub-processor to the controller, the controller, the processor, and the sub-processor must all agree. If direct notification of the controller by the sub-processor has been agreed, the processor must be informed by the sub-processor of each notification and provided with a copy of the notification. If notification of data breaches or data subject requests by the sub-processor to the processor has been agreed, the sub-processor has implemented processes to en- |

| | |
|---|---|
| | sure that the processor is notified. Communication channels and responsibilities must be defined for this. If no direct communication to the controller has been agreed, the sub-processor shall have implemented processes to ensure that the processor is notified (definition of responsibilities and communication channels, definition of what information is communicated to the processor).<br>3. The contract or other legal instrument under EU or German Law must be in writing pursuant to Art. 28 para. 9 GDPR, which may also be in an electronic format, see **DP07.09**.<br>4. Since the processor is obliged to provide the controller with all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR, the sub-processor must provide the processor with relevant information on how the processing activity is carried out (e.g., security concept, accountant reports, reports of the audit department or Data Protection Officer, or communication of the results of data protection audits or certifications). In addition, the sub-processor must allow for audits to be carried out by the processor itself or by an auditor appointed by the processor. Furthermore, the subprocessor must allow for audits to be conducted by the Controller itself or by an auditor appointed by the Controller.<br>5. The sub-processor must be obliged to ensure that processing by further sub-processors engaged by it is also carried out on the basis of a contract or other legal instrument in accordance with Union law or German law and that the same data protection obligations are imposed on them.<br>6. Processes are implemented to ensure that data processing by the sub-processor only takes place once the relevant processing agreement has been effectively concluded. At a minimum, the following is regulated:<br>• Documentation of how contracts are awarded (procurement channels/process)<br>• Guidelines for the commissioning of service providers (e.g. purchasing policy)<br>• Definition of responsibilities with regard to checking whether an data processing agreement must be concluded<br>• Determination of when data protection officers must be involved<br>• Existence of sample for a data protection agreement<br>• Determination of responsibilities with regard to the review of whether a data processing agreement GDPR must be concluded<br>• Definition of responsibilities for the conclusion of the data processing agreement (signature regulation)<br>• Documentation of the conclusion of the data processing agreement<br>• Documentation of the data processing agreement in accordance with established document management<br><br>**Engagement of additional sub-processors**<br>If the sub-processor engages another sub-processor, it must ensure that:<br>1. The controller must have given written, separate or general authorization to use the additional sub-processor, see **DP07.06**.<br>2. The sub-processor must impose the same data protection obligations on all additional sub-processors by means of a contract or other legal |

| | |
|---|---|
| | instrument under Union or German law as it has agreed with the processor, cf. the above comments and **DP07.09**.<br>3. The contract or other legal instrument under EU or German Law must be in writing pursuant to Art. 28 para. 9 GDPR, which may also be in an electronic format, see **DP07.09**.<br>4. The sub-processor only engages additional sub-processors who provide sufficient guarantees that appropriate technical and organizational measures will be implemented in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject., cf. **DP07.07.**<br>5. The sub-processor must ensure on an ongoing basis during the contractual relationship that sufficient guarantees are provided by the additional sub-processor, cf. **DP07.07.**<br>6. The additional sub-processor must be obliged to ensure that processing by further sub-processors employed by it is also carried out on the basis of a contract or other legal instrument in accordance with Union law or German law and that the same data protection obligations are imposed on them.<br>7. Specifications must be made regarding how the additional sub-processor must fulfill its support obligations pursuant to Art. 28 (3) (e) and (f) GDPR; see the above requirements.<br>8. Processes are implemented to ensure that data processing by the additional sub-processor only takes place once the relevant processing agreement has been effectively concluded. At a minimum, the following is regulated:<br>• Documentation of how contracts are awarded (procurement channels/process<br>• Guidelines for the commissioning of service providers (e.g. purchasing policy<br>• Definition of responsibilities with regard to checking whether an data processing agreement must be concluded<br>• Determination of when data protection officers must be involved<br>• Existence of sample for a data protection agreement<br>• Determination of responsibilities with regard to the review of whether a data processing agreement GDPR must be concluded<br>• Definition of responsibilities for the conclusion of the data processing agreement (signature regulation<br>• Documentation of the conclusion of the data processing agreement<br>• Documentation of the data processing agreement in accordance with established document management |

[GDPR] Art. 28 para. 3, 9 [GL2020-07] Section 1.3, 1.4

| | |
|---|---|
| **DP07.09** | **A) Controller**<br>The Controller has concluded a contract for order processing in accordance with Art. 28 GDPR with all Processors used in the context of IPS. All Processors used, including sub-processors, are documented.<br>In accordance with Art. 28 GDPR, the **contract for order processing** contains specific provisions on the processing of personal data by the Processor: |

| | |
|---|---|
| | 1. Object of the processing (Art. 28 para. 3 GDPR),<br>2. Duration of the processing (Art. 28 para. 3 GDPR),<br>3. Documentation of the type of processing (Art. 28 para. 3, Art. 28 para. 3 lit. a GDPR),<br>4. if applicable, the legal basis for the processing (Art. 28 para. 3 lit. a GDPR),<br>5. Obligation of the Processor to process data only on documented instructions - including in relation to the transfer of personal data to a third country or an international organisation - unless obliged to do so by EU or German law to which the Processor is subject; in such a case, the Processor must notify the Controller of these legal requirements prior to processing, unless the law in question prohibits such notification on grounds of important public interest (Art. 28 para. 3 lit. a GDPR)<br>6. Purpose of the processing (Art. 28 para. 3 GDPR),<br>7. Type of personal data processed (Art. 28 para. 3 GDPR),<br>8. Categories of data subjects (Art. 28 para. 3 GDPR),<br>9. Obligations and rights of the Controller (Art. 28 para. 3 GDPR),<br>10. Obligation of the authorised employees of the Processor to maintain confidentiality and secrecy or reference to any existing legal obligation to maintain confidentiality (Art. 28 para. 3 lit. b GDPR),<br>11. Taking all measures to ensure the security of processing in accordance with Art. 32 GDPR (Art. 28 para. 3 lit. c GDPR),<br>12. Specification that the Processor may not engage another processor without prior specific or general written authorisation of the controller. (Art. 28 para. 2 GDPR) and that the processor respects the conditions referred to in Art. 28 para. 2 and 4 GDPR for engaging of another processor (Art. 28 para. 3 lit. d GDPR),<br>13. Supporting the Controller in processing requests from data subjects (Art. 28 para. 3 lit. e GDPR),<br>14. Support of the Controller in the fulfilment of the obligations under Art. 32 to 36 GDPR by the Processor (Art. 28 para. 3 lit. f GDPR, more detailed requirements in the following criteria),<br>15. Deletion or return of the PD after completion of the provision of the processing services (Art. 28 para. 3 lit. g GDPR),<br>16. Provision of information to prove fulfilment of the obligations mentioned here (Art. 28 para. 3 lit. h GDPR),<br>17. Enabling and supporting audits to demonstrate compliance with the obligations mentioned here (Art. 28 para. 3 lit. h GDPR),<br>18. Information to be provided by the Processor to the Controller about the existence of an unlawful instruction (Art. 28 para. 3 sentence 3 GDPR).<br>The respective subject matter of the Processors (service description) is defined.<br>Processes have been implemented with regard to the selection and review of the Processors employed. The requirements of **DP07.05** apply in this regard. |

| | |
|---|---|
| | The contract or other legal instrument under European Union law or German Law must be in writing pursuant to Art. 28 para. 9 GDPR, which may also be in an electronic format. The contract or other legal instrument must be binding on the Processor in relation to the Controller, i.e. it must impose obligations on the Processor that are binding under European Union law or German law. It must also set out the obligations of the Controller.<br>Processes are implemented which ensure that data processing only takes place once the respective data processing agreement according to Art. 28 GDPR has been effectively concluded. This is regulated as a minimum:<br>• Documentation of how contracts are awarded (procurement channels/process)<br>• Guidelines for the commissioning of service providers (e.g. purchasing policy)<br>• Definition of responsibilities with regard to checking whether an data processing agreement according to Art. 28 GDPR must be concluded<br>• Determination of when data protection officers must be involved<br>• Existence of sample for a data protection agreement according to Art. 28 GDPR<br>• Determination of responsibilities with regard to the review of whether a data processing agreement according to Art. 28 GDPR must be concluded<br>• Definition of responsibilities for the conclusion of the data processing agreement (signature regulation)<br>• Documentation of the conclusion of the data processing agreement<br>• Documentation of the data processing agreement in accordance with established document management<br>The specification of the individual requirements can be found in the evaluation notes.<br><br>**B) Processor**<br>The Processor has concluded a contract for order processing in accordance with Art. 28 GDPR with all sub-processors used in the context of IPS. All sub-processors used are documented. The respective object of the Processor (service description) is defined.<br>In accordance with Art. 28 GDPR, the **data processing agreement** contains specific provisions on the processing of personal data by the Processor:<br>1. Object of the processing (Art. 28 para. 3 GDPR),<br>2. Duration of the processing (Art. 28 para. 3 GDPR),<br>3. Documentation of the type of processing (Art. 28 para. 3, Art. 28 para. 3 lit. a GDPR),<br>4. if applicable, the legal basis for the processing (Art. 28 para. 3 lit. a GDPR),<br>5. Obligation of the Processor to process data only on documented instructions - also with regard to the transfer of personal data to a third country or an international organisation (Art. 28 para. 3 lit. a GDPR) |

| | |
|---|---|
| | 6. Purpose of the processing (Art. 28 para. 3 GDPR),<br>7. Type of personal data processed (Art. 28 para. 3 GDPR),<br>8. Categories of data subjects (Art. 28 para. 3 GDPR),<br>9. Obligations and rights of the Controller (Art. 28 para. 3 GDPR),<br>10. Obligation of the authorised employees of the Processor to maintain confidentiality and secrecy or reference to any existing legal obligation to maintain confidentiality (Art. 28 para. 3 lit. b GDPR),<br>11. Taking all measures to ensure the security of processing in accordance with Art. 32 GDPR (Art. 28 para. 3 lit. c GDPR),<br>12. Specification that the Processor may not engage another processor without prior specific or general written authorisation of the controller (Art. 28 para. 2 GDPR) and that the processor respects the conditions referred to in Art. 28 para. 2 and 4 GDPR for engaging of another processor (Art. 28 para. 3 lit. d GDPR),<br>13. Supporting the Controller in processing requests from data subjects (Art. 28 para. 3 lit. e GDPR),<br>14. Support of the Controller in the fulfilment of the obligations under Art. 32 to 36 GDPR by the Processor (Art. 28 para. 3 lit. f GDPR, more detailed requirements in the following criteria),<br>15. Deletion or return of the PD after completion of the provision of the processing services (Art. 28 para. 3 lit. g GDPR),<br>16. Provision of information to prove fulfilment of the obligations mentioned here (Art. 28 para. 3 lit. h GDPR),<br>17. Enabling and supporting audits to demonstrate compliance with the obligations mentioned here (Art. 28 para. 3 lit. h GDPR),<br>18. Information to be provided by the Processor to the Controller about the existence of an unlawful instruction (Art. 28 para. 3 sentence 3 GDPR).<br>The respective operational implementation of the Processor must be described.<br>The Processor has implemented an audit-proof order management system, which includes in particular:<br>1. Documentation of the order processing procedures including the activities of other Processors,<br>2. Description of roles and interfaces,<br>3. Ensuring that the Data Processing Agreement is only concluded after the Data Processing Agreement has been concluded,<br>4. Logging of changes to the Processor.<br>The contract or other legal instrument under European Union law or German law must be drawn up in writing in accordance with Art. 28 para. 9 GDPR, which may also be in an electronic format.<br>The Processor has implemented processes for the selection and review of sub-processors. In this respect, the requirements of **DP07.07** apply. The persons authorised to process the PD at the Processor and at the sub-processors must be bound to confidentiality or be subject to a statutory duty of confidentiality. |

| | |
|---|---|
| | The contract or other legal instrument under EU or German Law must be in writing pursuant to Art. 28 para. 9 GDPR, which may also be in an electronic format. The contract or other legal instrument must be binding on the Processor in relation to the Controller, i.e. it must impose obligations on the Processor that are binding under European Union law or German law. It must also define the obligations of the Controller.<br><br>Processes are implemented which ensure that data processing only takes place once the respective data processing agreement according to Art. 28 GDPR has been effectively concluded. This is regulated as a minimum:<br>• Documentation of how contracts are awarded (procurement channels/process)<br>• Guidelines for the commissioning of service providers (e.g. purchasing policy)<br>• Definition of responsibilities with regard to checking whether an data processing agreement according to Art. 28 GDPR must be concluded<br>• Determination of when data protection officers must be involved<br>• Existence of sample for a data protection agreement according to Art. 28 GDPR<br>• Determination of responsibilities with regard to the review of whether a data processing agreement according to Art. 28 GDPR must be concluded<br>• Definition of responsibilities for the conclusion of the data processing agreement (signature regulation)<br>• Documentation of the conclusion of the data processing agreement<br>• Documentation of the data processing agreement in accordance with established document management<br><br>The specification of the individual requirements can be found in the evaluation notes. |

[GDPR] Art. Art. 28 para. 3 lit. a, Art. 29

| | |
|---|---|
| DP07.10 | **A) Controller**<br>Processing is always carried out on the **instructions of the Controller** - also with regard to the transfer of personal data to a third country or an international organisation. The procedure for issuing instructions must be agreed upon between the Controller and Processor. Verbal instructions must be followed up in writing (e.g. via e-mail). Persons authorised to issue instructions to the user and authorised recipients of the Processor are defined.<br>The specification of the individual requirements can be found in the evaluation notes.<br><br>**B) Processor**<br>Processing by the Processors, persons under their authority, and other processors is always carried out on the **instructions of the Controller** - also with regard to the transfer of personal data to a third country or an international organisation. Verbal instructions are followed up in writing. Instructions issued are documented and archived. Persons authorised to issue instructions at the user and authorised recipients of the Processor are defined. Processes are implemented to ensure that instructions are checked for data protection compliance (determination of responsibilities regarding the review of instructions, communication channels, determination of when data protection officers are to be involved).<br>If the Controller's instructions do not permit transfer or disclosure to third countries, the Processor may not commission a sub-processor in a third country with the processing, nor may it have the data processed in one of its departments outside the EU. The Processor must inform the Controller immediately if it believes that an instruction from the Controller violates the GDPR or other data protection regulations of the European Union or Germany.<br>The Processor must inform the Controller immediately if an instruction may violate data protection law. The Controller and communication channels for this must be documented.<br>The specification of the individual requirements can be found in the test notes. |

[GDPR] Art. 30

| | |
|---|---|
| DP07.11 | **A) Controller**<br>In accordance with Art. 30 para. 1 GDPR, the Controller must maintain a record of processing activities with the following contents:<br>1. Name and contact details of the Controller and, where applicable, the joint controller, the controller's representative and the Data Protection Officer,<br>2. Intended purposes of the processing (Art. 30 para. 1 lit. b GDPR),<br>3. Description of the categories of data subjects (Art. 30 para. 1 lit. c GDPR),<br>4. Description of the categories of personal data (Art. 30 para. 1 lit. c GDPR), |

| | |
|---|---|
| | 5. Categories of recipients to whom the IPS may disclose personal data (Art. 30 para. 1 lit. d GDPR),<br>6. where applicable, transfers of personal data to a third country or to an international organisation, including the identification of the third country or international organisation concerned and, for the transfers referred to in the second subparagraph of Art. 49 para. 1 GDPR, the documentation of appropriate safeguards,<br>7. deletion periods for the PD provided for in the IPS (Art. 30 para. 1 lit. f GDPR),<br>8. If applicable, a general description of special technical and organisational measures in accordance with Art. 32 GDPR that are required in connection with the use of IPS.<br>9. In the context of accountability, the respective legal bases are listed in the record of processing activities.<br><br>The record of processing activities must be checked regularly to ensure that it is complete and up to date. In the event of changes to the processing activities, it must be adapted so that it is up to date. Responsibilities for the regular review and adjustment of the record of processing activities must be defined. Changes to the register of processing activities must be documented and stored for at least one year (change history).<br>In accordance with Art. 30 para. 5 GDPR, there is no obligation to keep a record of processing activities for companies or organisations with fewer than 250 employees, unless the processing they carry out poses a risk to the rights and freedoms of the data subjects, the processing is not occasional or special categories of data are processed in accordance with Art. 9 para. 1 GDPR or the processing of personal data relating to criminal convictions and offences within the meaning of Art. 10 GDPR. If the Controller does not keep a record of processing activities due to the exception in Art. 30 para. 5 GDPR, it must be documented that none of the counter-exceptions actually apply. The specification of the individual requirements can be found in the audit notice.<br>In the case of joint controllership, each controller must maintain a record of processing activities in accordance with Art. 30 para. 1 GDPR. It must be indicated whether the respective processing activity is carried out under joint or sole controllership.<br><br>**B) Processor**<br>The Processor must maintain a record of processing activities in accordance with Art. 30 para. 2 GDPR with the following content:<br>1. the name and contact details of the Processor and of each Controller on whose behalf the Processor is acting and of any Data Protection Officer (Art. 30 para. 2 lit. a GDPR),<br>2. Categories of processing operations carried out on behalf of each Controller (Art. 30 para. 2 lit. b GDPR),<br>3. Where applicable, transfers of personal data to a third country or to an international organisation, including the identification of the third country or international organisation concerned and, in the case of transfers |

| | |
|---|---|
| | referred to in the second subparagraph of Art. 49 para. 1 GDPR, the documentation of appropriate safeguards (Art. 30 para. 2 lit. c GDPR),<br>4. if applicable, general description of special technical and organisational measures pursuant to Art. 32 GDPR that are required in connection with the use of IPS (Art. 30 para. 2 lit. d GDPR).<br>Changes to the register of processing activities must be documented and stored for at least one year (change history).<br>Pursuant to Art. 30 para. 5 GDPR, there is no obligation to keep a record of processing activities for companies or organisations with fewer than 250 employees, unless the processing they carry out poses a risk to the rights and freedoms of the data subjects, the processing is not occasional or special categories of data are processed pursuant to Art. 9 para. 1 GDPR or personal data relating to criminal convictions and offences within the meaning of Art. 10 GDPR are processed. If the Processor does not keep a record of processing activities due to the exception in Art. 30 para. 5 GDPR, it must be documented that none of the counter-exceptions actually apply.<br>The record of processing activities must be checked regularly to ensure that it is complete and up to date. In the event of changes to the processing activities, it must be adapted so that it is up to date. Responsibilities for the regular review and adjustment of the record of processing activities must be defined.<br>The specification of the individual requirements can be found in the test notes. |

## DP08 Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor must implement appropriate technical and organisational measures to ensure an appropriate level of security (see Art. 32 (1) GDPR). When assessing the level of protection, particular account must be taken of the risks associated with the processing, especially through the destruction, loss, alteration or unauthorised disclosure of or access to personal data that has been transmitted, stored or otherwise processed.

This section looks at the technical and organisational measures that must be implemented by the controller and the processor. If processors are used by the controller, it must be checked whether these processors have implemented appropriate technical and organisational measures.

If further sub-processors are used by the processor, it must be checked whether appropriate technical and organisational measures have also been contractually agreed for these sub-processors.

In order to assess whether appropriate technical and organisational measures have been taken, the risks to the rights and freedoms of data subjects with regard to data processing in the context of IPS must be taken into account. In this context, it is necessary to evaluate whether the processing operations have a risk or a high risk for the data subjects. The requirements for a risk analysis are listed below. Based on the identified risks to the rights and freedoms of natural persons, a assessment of protection needs (normal or high) must then be carried out. The standard requirements listed below (normal assessment of protection needs) or, in addition to the standard requirements, the requirements for increased protection needs (high assessment of protection needs) must be implemented.

When assessing the appropriateness of the implemented technical and organisational measures, it must be considered whether they correspond to the current state of the art. When assessing the state of the art, the evaluators are guided in particular by the recommendation on the state of the art, Federal Association for IT Security (current version), publications of the data protection supervisory authorities, publications of the Federal Office for Information Security (BSI) (e.g. technical guidelines, IT baseline protection compendium), publications of the European Network and Information Security Agency (ENISA).

Compliance with approved codes of conduct pursuant to Art. 40 GDPR can be used to demonstrate that appropriate technical and organisational measures have been taken to ensure a level of protection appropriate to the risk. Furthermore, recognised international certifications (e.g. DIN EN ISO / IEC 27000 series, BSI C5 etc.) can be used as proof. In this context, it must be evaluated whether the approved rules of conduct or the recognised international certification apply to the evaluation object.

[GDPR] Art. 32 para. 1 lit. d

| | |
|---|---|
| **DP08.01** | **Controller and processor**<br>The security level of the evaluation object and the effectiveness of the implemented technical measures must be verified by carrying out a penetration test (pentest) and documented in a test report.<br>The penetration test can be performed in the context of the evaluation or by a third party (third-party pentest). If a third-party pentest is submitted, the following requirements must be met.<br>• The pentest must have been carried out by a conformity assessment body authorised in accordance with DIN EN ISO/IEC 17025.<br>• The pentest must refer to the exact version of the evaluation object.<br>• The test report must clearly indicate the scope of the pentest or the components under consideration. All components/functions of the evaluation object must have been tested. |

| | |
|---|---|
| | • The test report must show how the test was carried out (manual/automated). Fully automated tests are not permitted.<br>• The test accounts/roles used must be documented.<br>• It must be clearly recognisable which test or attack procedures were used, so that it can be seen that at least all risks of the OWASP Top 10 catalogue were tested or were part of the tests / were taken into account.<br>In order to assess the implemented security measures of the evaluation object with regard to effectiveness and completeness and to identify risks, at least the following tests must be carried out in the context of the pentests:<br>a) Port and vulnerability scans<br>As part of port and vulnerability scans and thus tests at the network level, the relevant systems of the certification object are checked for the identified accessible services as well as IT vulnerabilities. The following steps or scans are performed:<br>▪ Determination of all network services that can be reached (from outside / from the Internet) by means of automated port scans (TCP and UDP protocols) of the target systems,<br>▪ SSL/TLS scan (for appropriately available services) to determine the SSL/TLS version and configuration in use,<br>▪ Automated vulnerability scans against the identified network services.<br>The results are then evaluated and verified to identify false-positive vulnerabilities/issues. In addition, publicly available sources (e.g., CVE databases) are used to identify information about potential vulnerabilities of the object of investigation or the services/software used (e.g., a web server).<br>b) Configuration analyses of systems and components<br>As part of configuration analyses, a manual examination is carried out at system or application level. The configuration analysis is carried out according to the white box approach. This means that (administrative) access to the system under investigation is a prerequisite. The configuration analyses are carried out together with the controller or processor. This requires unrestricted access to the systems and components. As part of the configuration analyses, security-relevant and possibly functional configuration settings must be viewed. Essentially, technical measures for system hardening, patch management, routing, logging, monitoring and, if applicable, cluster and virtualisation solutions are examined.<br>c) Application level penetration testing<br>The selected applications (e.g., mobile apps, web applications) are checked as part of penetration testing at the application level. The penetration test is performed as a combination of automated and manual tests. Fully automated tests are not permitted. As part of the automated tests, the test procedures in accordance with a) Port and vulnerability scans are used against the relevant systems of the evaluation object (e.g. the web server) in order to carry out checks at the network level. The Burp Suite Professionals tool is mainly used for the manual tests. |

| | |
|---|---|
| | The procedure is based on<br>• the implementation concept for penetration tests from the Bundesamt für Sicherheit in der Informationstechnik (BSI).<br>In addition, depending on the object of the evaluation<br>• the "Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks",<br>• the "OWASP Top 10 API Security Risks" and/or<br>• the "OWASP Mobile Top 10 Security Risks"<br>in the current version are taken into account and checks for these risks are carried out.<br>The associated tests are described in the OWASP Application Security Verification Standard (ASVS) and OWASP Mobile Application Security Verification Standard (MASVS).<br>The focus of the pentest is therefore on the following areas, depending on applicability:<br>• Injection / input and output validation<br>• Authentication (session management)<br>• Access control (authorisation) / client separation<br>• Data security / loss of confidentiality of sensitive data<br>• Security-relevant misconfiguration / lack of hardening<br>• Application logic<br>• Publication of security-relevant information / information disclosure<br>Depending on the specific characteristics of the respective object of investigation, special features or other key topics may be taken into account.<br>All results of the penetration test are made available in the form of a final report in German (alternatively in English). The results of the test are analysed, evaluated and prioritised.<br>Vulnerabilities that are categorised with a risk level of "medium" or higher prevent certification and must be remedied for successful certification. The risk analysis is carried out in accordance with the recognised BSI Standard 200-3. A risk category is defined for each vulnerability, which describes the criticality of the respective vulnerability. The overall risk is made up of the impact and the likelihood of occurrence. When assessing the risk levels, it must be noted that the specification of a risk level is always subjective. Unknown details or different interpretations of the security requirements can lead to an assessment that differs from the one given in this report.<br>A risk measurement plan must be drawn up for identified weaknesses, which must include at least the following:<br>• Technical and organisational corrective measures<br>• Prioritisation of risk treatment<br>• Responsibilities for implementation<br>• Deadlines for the implementation of remedial measures<br>• Documentation of when the measure was implemented |

| | |
|---|---|
| | • Status (date) of the risk action plan<br>The document history of the risk measurement plan must be kept for at least one year.<br>If the controller or processor remedies vulnerabilities that were identified during the initial penetration test, it must be proven by means of a re-test that these have been remedied. It must also be documented how they were remedied.<br>The results of the penetration test must be included in the established risk management process (see the requirements in **DP08.02**).<br>With regard to monitoring the effectiveness of the technical and organisational measures, regular penetration tests must continue to be carried out in addition to the mandatory proof of the penetration test. Appropriate planning must be in place for this, which in particular provides for<br>• Frequency of penetration tests<br>• Type of penetration test (internal or external)<br>• Scope of the penetration tests<br>• Responsibilities for carrying out the penetration test<br>• Processes for dealing with findings from the investigation, including the creation of a risk action plan (see above for content requirements)<br>With regard to determining the frequency of the penetration test, the following standard applies: If, as part of the systematic analysis of possible risks to the protection of personal data resulting from their processing with the IPS, the determination of protection requirements comes to the result “high” (see **DP08.02**), penetration tests must be carried out at least once a year or on an ad-hoc basis (e.g. in the event of security-relevant changes to the IT infrastructure, known security incidents or increased risk due to the threat situation). In the case of normal protection requirements, penetration tests must be carried out every two years or as required (e.g. in the event of security-relevant changes to the IT infrastructure, known security incidents or increased risk due to the threat situation). |

[GDPR] Art. 32 para. 1,

| | |
|---|---|
| DP08.02 | **Controller and Processor**<br>The technical and organisational measures provided for in connection with the operation of the IPS are based on a systematic **analysis of possible risks** to the protection of personal data resulting from their processing with the IPS.<br>The processes of risk identification, risk assessment and risk treatment must be documented in a systematic procedure that is carried out regularly and is based on standardised procedures for risk management ([BSI-200-3], [ISO 31000], [ISO/IEC 27005], [ISO 14971]). Risk management must fulfil the following requirements:<br>1. The risk management processes must be run through regularly (at least annually) and adjusted if necessary, particularly in the event of changes to risks. Those responsible for risk management must approve the risk assessment and risk treatment, including the acceptance of residual risks.<br>2. risk identification: Relevant sources of risk must be systematically identified. This involves determining which events (causes) could lead to a specific event and which circumstances or actions could cause this to occur. The risk scenarios must be as specific as possible. The entire processing cycle must be taken into account when identifying risks.<br>3. risk analysis: During the risk analysis, the following parameters must be determined for each identified risk:<br>• Type of processing including categories of personal data<br>• Scope of processing: The amount of personal data and the number of data subjects whose data is processed must be taken into account.<br>• Circumstances of the processing: In particular, the parties involved in the processing, the place and duration of processing, the source of the data and the type of collection must be taken into account<br>• Purpose of processing: This requires a clearly defined purpose.<br>4. risk assessment and risk treatment: For the risk assessment, the possible risk levels (combination of probability of occurrence and extent of damage) must be defined in a risk matrix. Appropriate risk acceptance criteria must be defined for risk treatment. The selection of risk-mitigating measures must be based on the IT baseline protection compendium of the BSI, implementation instructions of ISO/IEC 27002 and the catalogue of measures of the standard data protection model. The following parameters must be determined for each analysed risk:<br>• Probability of occurrence,<br>• Extent of damage (with regard to the rights of data subjects)<br>• Risk level according to the defined risk matrix<br>• assessment of protection needs (normal or high)<br>• Risk owner<br>• Planned risk-minimising measures<br>• Residual risk after implementation of risk-minimising measures<br>• Data protection impact assessment<br>If the assessment of the need for protection reveals a high need for protection, the requirements for a high protection requirement must be |

| | |
|---|---|
| | met in addition to the standard technical and organisational requirements from sections **DP08.01, 08.03 to DP08.05**.<br>The results of penetration tests carried out (risk identification, risk analysis, risk assessment and risk treatment) must also be taken into account as part of established risk management, cf. **DP08.01**.<br>In the context of the assessment of protection needs, it must be evaluated whether a data protection impact assessment (DPIA) must be carried out in accordance with Art. 35 GDPR, cf. the requirements in **DP10**.<br>The technical and organisational measures implemented are to be documented in a data security concept. The data security concept must at least include regulations on:<br>• Roles and responsibilities<br>• Scope of application<br>• Measures to ensure confidentiality (admission control, access control, access control, separation control, pseudonymisation, encryption)<br>• Measures to ensure integrity (transfer control, input control)<br>• Measures to ensure availability and resilience<br>• Procedures for regular review, assessment and evaluation<br>• Review and update of the data security concept<br>The data security concept must be regularly reviewed to ensure it is up to date (at least annually or when changes are made) and further developed.<br>**Addendum for processors**<br>If the controller is responsible for the implementation of individual technical and organisational measures, the processor must inform the controller about this. Appropriate documentation must be available for this purpose. |

[GDPR] Art. 25 para. 1, 2, [GDPR] Art. 32 para. 1 lit. a, b

| | |
|---|---|
| **DP08.03** | **Controller and Processor**<br>The controller and processor must take appropriate technical and organisational measures to ensure the confidentiality of the processed personal data, taking into account the state of the art.<br>It must also be ensured that the processors or sub-processors used have also implemented these measures.<br>The following standard requirements for the confidentiality of the processed PD must be implemented. If the assessment of protection needs reveals a high need for protection, the requirements for increased protection needs must be met in addition to the standard requirements.<br>**1. Access control measures**<br>The controller and processor must have established access control mechanisms to ensure that access to buildings and premises as well as access to the IPS is prevented for unauthorised persons.<br>**Standard requirements:**<br>1. security concept: |

| | |
|---|---|
| | a. A concept for access regulations and physical access control (perimeter protection) for offices, rooms and facilities must be documented and implemented.<br>b. Security areas with physical access controls must be defined.<br>2. structural safety measures:<br>a. Fire protection measures (fire and smoke detectors, fire alarm system, extinguishing system, etc.) must be taken.<br>b. Cables that transport power or data must be protected against interception, interference or damage.<br>3. key management and means of access:<br>a. There must be a documented regulation for physical key management.<br>b. The issue and withdrawal of access resources such as chip cards and keys must be documented.<br>c. Access media that have been compromised or lost must be replaced or blocked.<br>4. dealing with visitors and external service providers:<br>a. There must be rules for dealing with visitors. In secure areas, visitors must be accompanied by an authorised person at all times.<br>b. Arrangements must be made for external service providers, such as confidentiality agreements and personal support.<br>5. checking and updating access authorisations:<br>a. Access authorisations must be checked regularly to ensure that they are up to date and appropriate and updated if necessary.<br>b. Access authorisations must be temporarily blocked in the event of prolonged absences.<br>c. There must be multi-factor authentication for access to data processing systems.<br>6. logging:<br>a. There must be a log of physical access to premises in secure areas or with data processing systems.<br>**Requirements for increased protection needs:**<br>7. structural safety measures:<br>a. Measures such as fencing, video surveillance, burglar-proof doors and windows are required. The design of these measures must take into account the risk to the rights and freedoms of those affected.<br>8. logging:<br>a. Any unauthorised access or attempted access must be logged and must be detectable at a later date.<br><br>**2. Access control and identity and authorisation management**<br>The controller and processor must have established an identity and authorisation management system that ensures that unauthorised persons do not have access to the IPS. The processes and measures for identity and authorisation management must be based on the state of the art ([ BSI IT-Grundschutz-Kompendium ORP.4 Identitäts- und Berechtigungsmanagement], [ISO 27002 Clauses 5.15 - 5.18]).<br>**Standard requirements:** |

| | |
|---|---|
| | 1. authorisation concept:<br>a. The authorisation concept must document all access and access to services and systems that process personal data.<br>b. All access and access to services and systems that process personal data must have passed an authorisation check and be clearly identifiable.<br>c. The controller/processor must document procedures for assigning, checking, enforcing and deleting authorisations for access, entry and access rights in an authorisation concept.<br>d. Authorisations must be assigned and changed on the basis of the principle of least privilege and as required for the performance of tasks ("need to know principle").<br>e. The controller/processor must define and document roles and authorisations.<br>f. The tasks and functions of administration roles and user roles must be clearly separated.<br>g. Responsibilities for the procedures for assigning, checking, enforcing and deleting authorisations must be defined.<br>h. Changes to authorisations for access and access to services and systems that process personal data must be approved by superiors or responsible persons.<br>i. The assignment, verification, enforcement and cancellation of rights and authorisations must be documented.<br>j. Authorisation management must include access and access to relevant systems by employees of processors.<br>2. management of access and authorisations:<br>a. Saving, editing, deleting and accessing authorisations and the associated access authorisations must be carried out via administrator accounts or user accounts with elevated rights.<br>b. All users and user groups are set up and deleted exclusively via separate administrative roles.<br>c. User accounts that are not required, such as guest accounts or standard administrator accounts, must be blocked or deleted.<br>d. Group user accounts must be avoided.<br>e. When using group user accounts, there must be a data protection-compliant logging of the associated user activities.<br>f. In the event of personnel changes, user accounts and authorisations that are no longer required must be removed.<br>3. handling of physical data:<br>a. Secure locking systems including documented key management must be used for physical files and data.<br>4. checking and updating access and authorisations:<br>a. Inactive user accounts must be identified and blocked or deleted.<br>b. The controller/processor must check the necessity of the authorisations for access to rooms and facilities, access |

and access to the IPS and backup copies at regular intervals to ensure that they are up to date and appropriate and update them if necessary.

5. machine-to-machine communication:
   a. Machine-to-machine communication must be secured for relevant data processing operations via mutual authentication mechanisms.
   b. The communication channel between the authenticated server and the client must be encrypted in accordance with the requirements in the crypto concept.

**Requirements for increased protection needs:**

6. logging:
   a. Every change and deletion of authorisations for access and access to services and systems that process personal data must be logged and subsequently identifiable.
   b. The controller/processor takes measures to actively detect unauthorised changes and attacks on authorisation systems and assigned authorisations.
   c. Logging processes and activities on administrative IT systems must be recorded.
   d. Administrators must not have the ability to change or delete log files about their own activities with their administrator accounts.
7. confidential data processing:
   a. The principle of dual control must be applied for administration activities. In the case of data processing systems, a single administrator alone may not gain access to the data processed on the server.

**3. Access control measures**

The controller and processor must have established access control mechanisms to ensure that unauthorised persons cannot access the IPS and personal data.

**Standard requirements**

1. general requirements:
   a. Networks must be segmented to make it more difficult for unauthorised persons to access the IPS, relevant systems and personal data.
   b. Procedures for blocking data in the event of suspected unauthorised access must be implemented.
2. logging and monitoring:
   a. All access to personal data must be logged.
   b. Access to data backups must be restricted to authorised persons.
   c. Access protection for personal data on mobile devices must also be guaranteed in the event of loss or theft.
   d. The Controller must take protective measures against known attack scenarios in relation to access violations.
3. remote access:

a. Remote access to the IPS or personal data via the Internet or other insecure networks must provide for the use of a virtual private network (VPN) and measures to encrypt the data streams in accordance with the crypto concept.
b. A list of users or user categories with remote access must be created.

**Requirements for increased protection needs:**

4. logging:
   a. Every unauthorised access and every access attempt must be logged and subsequently detectable.

**4. Authentication and authorisation**

**Standard requirements:**

1. authentication concept:
   a. The controller/processor must create an authentication concept in which the authentication requirements are defined for each relevant IT system and each relevant application.
2. password policy:
   a. The controller and processor must regulate the use of authentication means (passwords, etc.) in a binding manner.
   b. The password policy must specify which users and user groups are subject to multi-factor authentication for access to the IPS.
   c. Multifactor authentication must be used for users with administrator accounts, users with access to sensitive data in accordance with the GDPR and users with remote access via a virtual private network.
   d. A procedure for assigning passwords must be documented.
   e. Minimum requirements for the complexity of passwords must be defined, taking into account the state of the art.
   f. A procedure for resetting and blocking passwords must be implemented.
   g. Rules for handling passwords must be documented.
   h. Employees must be instructed in the use of authentication procedures and mechanisms.
   i. Employees must be sensitised to the use of authorisation-tools such as passwords. This applies in particular to the inadmissibility of passing them on, the inadmissibility of multiple use and the unreliability of documenting passwords on a piece of paper.
3. password management:
   a. Default passwords must be changed when logging in for the first time or after resetting the password.
   b. Passwords must be renewed regularly for administrator accounts.
4. password complexity:

| | |
|---|---|
| | a. The password complexity for exclusive password authentication must have an entropy of at least 80 bits (e.g. 12 characters with upper case letters, lower case letters, numbers and special characters).<br>b. The password complexity for password authentication with access restrictions, the entropy of the password must be at least 50 bits (e.g. 8 characters with all character categories).<br>c. The password complexity for password authentication with possession factor and access blocking after failed attempts must have an entropy of at least 13 bits.<br>5. technical measures for systems:<br>a. The systems must not issue any specific notifications in the event of unsuccessful login attempts.<br>b. Strong, state-of-the-art passwords must be technically enforced.<br>c. Measures must be implemented to recognise the compromise of passwords.<br>d. To prevent brute force attacks on passwords, there is:<br>1. a delay in accessing the account after several failed attempts, the duration of which increases exponentially with the number of attempts within a certain period of time; or<br>2. a mechanism that sets a maximum number of authorised attempts within a given time period, with a maximum of 10 attempts per hour; or<br>3. a blocking of the user account after a maximum of 10 consecutive failed authentications, with a release mechanism.<br>e. Systems must log failed authentication attempts.<br>6. protection of authentication factors:<br>a. Sending and storing passwords in plain text must be prevented.<br>b. Passwords must be stored using cryptographic hash functions.<br>**Requirements for increased protection needs:**<br>-<br><br>**5. Cryptography**<br>**Standard requirements:**<br>1. crypto concept<br>a. A cryptographic concept must be available that documents the encryption algorithms to be used for encryption, the duration of use of the cryptographic procedure and the associated key lengths.<br>b. Encryption must already be used as a protective measure at low risk. |

| | |
|---|---|
| | c. The encryption methods and key lengths used must correspond to the state of the art [BSI-TR-02102-01, -02, -03, -04].<br>d. The encryption methods used must not have any known security vulnerabilities.<br>e. Key management measures must be documented and implemented.<br>f. Technical developments in the field of encryption must be constantly monitored.<br>g. The Controller regularly reviews the crypto concept and updates it if necessary.<br>2. key management<br>a. Rules must be defined for the creation, renewal, exchange, destruction and storage of keys.<br>b. Cryptographic keys must be generated with suitable key generators and in a secure environment.<br>c. In hardware or software with cryptographic functions, preset keys (except public certificates) must be replaced<br>d. Secret keys must be stored securely and protected against unauthorised access.<br>e. Long-lasting cryptographic keys must be stored offline, outside the IT systems used.<br>f. A procedure must be defined in the event that a private key is disclosed.<br>3. transport encryption<br>a. State-of-the-art transport encryption must be used for data transmission processes.<br>b. The processing of encrypted data must be enabled as far as technically possible.<br>4. encryption of stored data<br>a. Login data for the use of systems and services must be stored in encrypted form.<br>b. Personal data must be stored in encrypted form.<br>5. documentation<br>a. The implementation of the encryption procedures must be documented.<br>**Requirements for increased protection needs:**<br>6. crypto concept<br>a. The company must check at least once a year whether the cryptographic procedures used and the associated parameters are still secure and have no known vulnerabilities.<br>b. A procedure must be defined for authorised physical access to hardware with cryptographic functions, e.g. for maintenance purposes.<br>7. key management<br>a. Hardware and software with cryptographic functions and keys must be monitored for manipulation attempts and it must be possible to detect any attempts retrospectively.<br>b. The configuration of the cryptographic hardware must be checked regularly.<br>8. test of the encryption methods |

a. The suitability of the encryption methods must be continuously checked and tested.

**6. Separation**

**Standard requirements:**

1. general requirements:
   a. The controller/processor processes the system client's data logically or physically separately from the data stocks of other system clients.
   b. The controller/processor enables the system customer to separate the data processing according to different processing purposes.
   c. The controller/proecssor must prevent breaches of data separation caused by technical or organisational errors, including operating errors, or negligent actions by employees or users.
   d. The controller/processor must be able to recognise intentional violations of the separation requirement.
   e. There must be a separation of development, testing and production environments during development.
   f. In the case of IT systems, the test environment must be separated from the production environment.
2. client separation:
   a. A client separation concept must be created and implemented.
   b. The client separation concept must ensure that data and processing contexts of different users are separated securely.
   c. A distinction must be made between client-specific and cross-client data.
   d. The required mechanisms for client separation must also be implemented by service providers in the case of relevant data processing.

**Requirements for increased protection needs:**

1. extended protective measures:
   a. The Controller/processor must take measures before known attack scenarios against the separation.
   b. Encryption of data storage from different customers must be carried out with (customer) individual keys.

**7. Pseudonymisation**

The use of pseudonymisation must be based on the state of the art ([EDPB Guidelines[3] ], [ISO 27002]).

**Standard requirements:**

general requirements:

a. The use of pseudonymisation or anonymisation must be carried out depending on the assessment of protection needs and the use of the data.

[3] https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

| | |
|---|---|
| | b. The controller must take measures to ensure that pseudonymised or anonymised data is not compared with other information without authorisation in order to identify individuals.<br>1. <u>separate processing:</u><br>a. Pseudonymised data and additional information that enables re-identification must be processed separately.<br>b. When pseudonymising personal plain text data using cryptographic procedures, the controller or processor must ensure that the cryptographic key is stored separately to restore the personal reference.<br>c. The separate storage of keys can take place at a logical level (e.g. through authorisation concepts), but also at a physical level (e.g. through dedicated data processing systems) or at an organisational level (e.g. through a data trustee).<br>**Requirements for increased protection needs:**<br>- <br><br>**<u>Addendum for processors</u>**<br>Processors must ensure in accordance with Art. 28 para. 3 lit. c GDPR that all measures required in accordance with Art. 32 GDPR are taken and that the data security requirements are implemented in accordance with the agreement concluded with the controller. To this end, the agreement between the controller and the processor must contain information on the following points<br>▪ The technical and organisational measures to be taken<br>▪ Obligation of the processor to agree significant changes to the technical and organisational measures with the controller (in writing or electronically) and to retain them for at least the duration of the agreement<br>▪ Regular review of technical and organisational measures<br>The controller must provide the processor with a description of the processing activities and the security objectives (based on the controller's risk assessment) and approve the technical and organisational measures proposed by the processor.<br>The information on the technical and organisational measures implemented by the processor must be detailed to enable the controller to check the appropriateness of the measures in accordance with Art. 32 (1) GDPR.<br>The processor must have implemented procedures to regularly review, assess and evaluate the effectiveness of the technical and organisational measures. The implemented procedures must at least define:<br>▪ The responsibilities regarding the regular review, assessment and evaluation of the technical and organisational measures.<br>▪ Time cycles for the regular review of technical and organisational measures (at least every two years). In addition, it must be determined when checks are to be carried out without cause, e.g. in the event of technical changes such as software updates or the discovery of new attack methods. |

| | |
|---|---|
| | ▪ the manner of the review.<br>▪ Carrying out a review of the specific technical and organisational measures implemented by the respective controller<br>▪ Carrying out a comparison with the security objectives and the corresponding level of protection. Assessment of whether the technical and organisational measures ensure the level of protection. Adjustments to the security objectives due to changes in the circumstances and framework conditions of the processing itself, any updates or security gaps that have become known must also be taken into account and it must be evaluated whether further risks have arisen that require an adjustment of the measures.<br>▪ Evaluating the effectiveness of technical and organisational measures, e.g. through penetration tests.<br>▪ The verifications carried out must be documented.<br>If the measures taken by the processor do not meet the requirements of the controller, the controller must be informed of this immediately (in written form, including electronically). Appropriate processes, including responsibilities and communication channels, have been defined for this purpose. |

[GDPR] Art. 25 para. 1, 2, [GDPR] Art. 32 para. 1 lit. b, c

| | |
|---|---|
| **DP08.04** | **Controller and Processor**<br>In connection with the operation of the IPS, the controller and processor must take technical and organisational measures to ensure the **availability** of the processed personal data, taking into account the state of the art. The processes and measures must be based on standardised procedures for continuity management and the state of the art ([BSI-200-4], [BSI IT-Grundschutz-Kompendium], [ISO 22301]). The following standard requirements for the availability of the processed PD must be implemented.<br><br>**Standard requirements:**<br>1. data backup strategy and concept:<br>a. There must be a data backup concept that describes the regular data backup of relevant systems, configurations, data structures and transaction histories, as well as the requirements for storage and physical and logical protection.<br>b. The data protection concept must provide an overview of which IT systems and which data on them are backed up and how.<br>c. The order in which the IT systems and applications are restored must be defined.<br>d. The data backup concept must describe the regular review of the recoverability of backup copies.<br>2. data backup plans:<br>a. Data backup plans must be created for relevant IT systems or groups of IT systems.<br>b. The following aspects must be defined in the backup plans:<br>1. the database to be backed up,<br>2. Requirements for the data backup archive, |

| | |
|---|---|
| | 3. Data confidentiality requirements,<br>4. Use of encryption techniques,<br>5. the number of data backups,<br>6. required storage volume,<br>7. the type of data backup,<br>8. Frequency and time of data backup,<br>9. the storage medium,<br>10. Checking the database and the storage medium to be used for malware<br>11. prior secure deletion of the data carriers before re-use,<br>12. the storage location (physical, logical) of the data backup,<br>13. the hardware and software used for data backup,<br>14. Responsibility for data backup,<br>15. Transport and storage modalities,<br>16. Documentation of the backups created (date, type of backup and selected parameters, labelling of the data carriers)<br>c. The data backup plans must take into account data retention and deletion periods.<br>d. There must be user documentation for carrying out the data backup and restoring data from the data backup.<br>3. framework conditions for data backup:<br>a. Sufficient hardware resources must be available for data backup.<br>b. Data backups must not be permanently connected to the IT network, but only during the data backup or restore process.<br>c. Employees must be informed and, if necessary, trained about their data backup tasks.<br>4. secure storage:<br>a. Data storage medium must be stored separately from the secured IT system.<br>b. Climatic conditions for the long-term storage of data storage medium must be guaranteed.<br>c. Access to and use of data storage medium with data backups must only be possible for authorised persons.<br>d. IT systems used for data backup may only allow write access to the storage media for data backup for authorised data backups or authorised administration activities.<br>e. Buildings or premises with relevant systems for data processing must be equipped with appropriate protective measures against elementary threats such as fire, water, lightning and electromagnetic fields.<br>f. The availability of the data and the IPS must be ensured in the event of short-term power failures.<br>5. cloud data backups:<br>a. There must be a contract with the service provider that specifies the location of data storage, service level agreements (SLA), technical and organisational measures.<br>b. There must be suitable authentication methods according to the state of the art. |

| | |
|---|---|
| | c. The encryption of data in transit and in online storage must be state of the art.<br>6. function tests and verification of recoverability:<br>a. Regular tests of the data backups must be carried out.<br>b. When testing the data backups, it must be ensured that the data backup is complete and that the data can be used after restoration.<br>c. If necessary, fast access or access to the data backups must be guaranteed.<br><br>**Requirements for increased protection needs:**<br>7. data backup strategy and concept:<br>a. The data backup concept must define restart and recovery times.<br>8. data backup plans:<br>a. Data backups must be carried out according to the 3-2-1 rule or an adequate principle: 3 data storage locations, 2 different backup media (also "offline" such as tape backups) and 1 of these at an external location.<br>9. secure storage:<br>a. Data carriers must be stored separately from the secured IT system, in a different fire compartment.<br>10. encryption:<br>a. It must be ensured that the encrypted data can be restored even after a longer period of time.<br>b. Cryptographic keys used must be protected with a separate data backup.<br>11. function tests and verification of recoverability:<br>a. The regular tests of the data backups must check whether the defined times for restarting and restoring are adhered to in accordance with the data backup concept.<br>12. redundancies:<br>a. Redundancies must be available for the IPS to ensure that access to the IPS and personal data is as uninterrupted as possible.<br>13. procurement of data backup systems:<br>a. Before a data backup system is procured, the IT organisation must draw up a list of requirements according to which the products available on the market are evaluated.<br>The data backup systems purchased must fulfil the requirements of the company's data backup concept. |

[GDPR] Art. 25 para. 1, 2, [GDPR] Art. 32 para. 1 lit. b,

| | |
|---|---|
| **DP08.05** | **Controller and processor**<br>In connection with the operation of the IPS, the controller and processor must take technical and organisational measures to ensure the **integrity** of the processed personal data, taking into account the state of the art. The following standard requirements for the integrity of the processed personal data must be implemented. If the assessment of protection needs reveals a high protection need, the requirements for the high protection |

| | |
|---|---|
| | need must be met in addition to the standard requirements.<br><br>**Standard requirements:**<br>1. <u>general requirement:</u><br>a. There must be a documented process for selecting and implementing technical and organisational measures to ensure the integrity of data processing (determination of responsibilities, criteria for selecting technical and organizational measures, documentation of technical and organizational measures).<br>b. The controller/processor must document and implement procedures as soon as breaches of the integrity of processed data are recognised or reasonably suspected.<br>c. These procedures must include the blocking or deletion of data for which sufficient integrity cannot be determined to meet the protection requirements.<br>d. Mechanisms must be put in place to prevent or detect unauthorised or unintentional modifications to stored or transmitted data.<br>e. Mechanisms must be put in place to ensure that data is up to date.<br>f. Mechanisms must be set up to ensure data consistency.<br>g. The integrity of the algorithms used for PD must be protected.<br>h. The controller/processor must protect the transport of data carriers so that personal data cannot be read, copied, modified or removed without authorisation during transport.<br>2. <u>logging:</u><br>a. The controller/processor must log entries, changes and deletions of personal data. A record must also be kept of who made the changes and when this was done.<br>b. It must be documented how, where (which IT system) and what is logged. The type and scope of logging must be based on the need for protection.<br>c. The controller/processor must observe the principles of necessity, purpose limitation, data minimisation and storage limitation when keeping logs. When determining the storage period, the purpose pursued and the existing risk must be taken into account. The respective storage period must be documented and it must be explained why it is considered necessary (e.g. in the record of processing activities). After the storage period has expired, the log data must be deleted. The procedure for erasure must be documented. When logging deletion processes for log data, no personal data may be included in the contents of the deletion log. Instead, references to file numbers or file names must be included if necessary.<br>d. The logging must be designed in such a way that it can be analysed.<br>e. The logging must be designed in such a way that the traceability of entries, changes and deletions is maintained even in the event of technical or organisational errors, including |

| | |
|---|---|
| | operating errors by users or employees.<br>f. Log data must be stored securely, i.e. it must be ensured that altered access is not possible, it must be ensured that only authorised persons have accessa<br>g. The logging data must be checked regularly, e.g. by the information security officer.<br>h. Access to log data must be documented.<br>i. Administrative activities must be recorded.<br>3. <u>data backup and malware protection:</u><br>a. The controller/processor must set up procedures for analysing and checking logs in order to effectively detect anomalies and incidents and subsequently trigger an alarm.<br>b. The controller/processor must ensure that the integrity of personal data is also guaranteed in data backups.<br>c. The Controller/processor must ensure that no changes or manipulations were made to the data when it was restored.<br>4. <u>use of cryptographic procedures:</u><br>a. Encryption procedures must be used for the transport of data and remote access to data in accordance with the assessment of protection needs.<br>b. State of the art encryption methods [BSI-TR-02102-01, -02, -03, -04] must be used for encryption.<br>**Requirements for increased protection needs:**<br>5. <u>use of cryptographic procedures:</u><br>a. If, according to the assessment of protection needs, the PD has a high protection requirement, the data must be encrypted.<br>b. To ensure the integrity of backed-up data, all data backups must be encrypted.<br>6. <u>tamper protection and protection against malware:</u><br>a. The controller/processor must take measures to actively detect tampering with logging instances and files and to defend against attacks, and must subsequently detect any unauthorised reading, copying, modification or removal of data and any attempt to do so. |

[GDPR] Art. 32 para. 1 lit. d

| | |
|---|---|
| DP08.06 | **Controller and Processor**<br>The controller and the processor maintain **procedures for the regular review**, assessment and evaluation of the technical and organisational measures, taking into account the further development of the state of the art and the requirements of data protection.<br>In particular, evidence must be provided for the following:<br>▪ Regular internal audits/reviews in the area of data protection and IT security. A test plan must be in place for this. The plan must, in particular, specify:<br>o o Responsibilities for the audit<br>o o Type of audit<br>o o Scope of the audit<br>o o Timetable for the audit<br>The audits must be documented.<br>▪ event-driven checks, e.g. when technical changes such as software updates are made or new attack methods become known.<br>▪ Processes for reviewing and updating the data security concept, taking into account changed security requirements and possible changes to the risk assessment (see DP08.01 and DP08.02)<br>▪ Contact with authorities and interest groups to stay informed about current threats and available countermeasures, and to be able to take them into account in a timely and appropriate manner<br>o Processes (responsibilities, communication channels) are in place to communicate this information to the relevant employees.<br>▪ Review of updated software and IT procedures according to a test plan (cf. DP09.07)<br>▪ If applicable, availability certifications in the field of IT security<br>Implementation of attack scenarios at appropriate intervals (e.g. pentests, cf. DP08.01) |

[GDPR] Art. 32

| | |
|---|---|
| DP08.07 | **Controller and processor**<br>**Responsibilities for the security of processing** (e.g. IT security officer, data protection officer) are defined for the operation of the IPS. |

## DP09 Data protection management

[GDPR] Art. 33, Art. 28 para. 3 sentence 2 lit. f

| | |
|---|---|
| DP09.01 | **A) Controller**<br>In the event of a **personal data breach,** the Controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, see Art. 33 para. 1 sentence 1 GDPR.<br>With regard to the handling of personal data breaches, processes are in place with clear procedures, guidelines regarding risk assessment (responsibilities and procedures) and responsibilities for reporting to the supervisory authority.<br>These include:<br>1. documentation of data breaches, their effects and the corrective measures taken,<br>2. responsibilities for assessing the risk of a personal data breach to the rights and freedoms of natural persons<br>3. processes and methods for assessing the risk of a personal data breach<br>4. responsibilities regarding the assessment of whether there is an obligation to report a personal data breach to the competent supervisory authority<br>5. responsibilities and procedures for reporting to the competent supervisory authority, taking into account the 72-hour period to be observed, if a reporting obligation exists.<br>The Controller has established a process for dealing with **information security incidents** and considers whether the personal data breach is caused by an information security incident. The Controller must at least consider the following aspects when dealing with information security incidents:<br>1. Mechanisms and a contact point are in place to enable employees to report incidents, breaches or vulnerabilities via established channels. Roles for dealing with information security incidents are defined and communicated to relevant parties. It must be ensured that specially trained personnel are responsible for handling information security incidents and have access to the relevant process documentation.<br>2. Definition and categorisation of information security incidents<br>o information security incidents are effectively categorised and prioritised. Following this categorization scheme, it must be possible for each information security event to be assessed by the responsible personnel using a defined scheme. The assessment must be documented.<br>3. Ensuring that information security incidents are responded to and assessed. The following aspects must be taken into account:<br>o Limiting the spread of the incident to other systems |

| | |
|---|---|
| | ○ Collecting evidence related to the information security incident<br>○ Identification and elimination of vulnerabilities<br>○ Consideration of any existing business continuity plans<br>○ Carrying out (forensic) information security analyses<br>4. The knowledge gained from the previous analysis of the incidents must lead to an optimisation of the incident management processes and must be considered in the risk analysis.<br>5. New or recurring security incidents must be prevented by creating monitoring processes. Continuous logging and monitoring of security-relevant activities and anomalies within the networks, systems and applications can serve this purpose.<br>**B) Processor**<br>There is a contractual obligation to support the Controller in the event of a data breach notification. The Processor has implemented and documented processes to ensure that data breaches are recognised and investigated in a timely manner (establishment of reporting channels, definition of responsibilities regarding the handling of data breaches, as well as the implementation of mitigation measures, documentation of the data breach). In addition, the Processor has implemented and documented processes to ensure that the Controller is informed of the data breach without delay, see Art. 33 para. 2 GDPR (determination of responsibilities and communication channels, determination of what information is communicated to the controller).<br>The Processor supports the Controller, taking into account the nature of the processing and the information available to it, in reporting personal data breaches to the supervisory authority, see Art. 28 para. 3 sentence 2 lit. f GDPR.<br>The Processor also has a process in place that regulates the handling of information security incidents (establishment of reporting channels, definition of responsibilities regarding the handling of information security incidents, including implementation of mitigation measures, documentation of the information security incident). The Processor takes technical measures that can effectively recognise security incidents and trigger an alert. The process provides for notification of a security incident to a Controller (determination of responsibilities and communication channels, determination of what information is communicated to the controller). The Processor ensures that information security incidents are responded to and analysed. The results of the analysis must be made available to the Controller. |

[GDPR] Art. 34, Art. 28 para. 3 sentence 2 lit. f

| | |
|---|---|
| **DP09.02** | **A) Controller**<br>A process is in place to ensure that, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subject is notified without undue delay. Processes (determination of responsibilities and communication channels regarding notification of data subjects) and methods for risk assessment of the personal data breach are implemented, see **DP09.01**. It is ensured that the information |

| | |
|---|---|
| | about the nature of the personal data breach is provided in clear and plain language. The information contains at least the following details:<br>1. Name and contact details of the Data Protection Officer or other point of contact for further information,<br>2. Description of the likely consequences of breaching the PD protection,<br>3. A description of the measures taken or proposed to be taken by the Controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.<br>Notification of the data subjects is not required if one of the following conditions is applicable (see Art. 34 para. 3 GDPR)<br>1. the controller has taken preventive security measures that were applied to the affected PD in advance of the data breach and prevent unauthorised access to the data (e.g. through appropriate encryption);<br>2. the initially assumed high risk no longer exists due to the subsequent measures taken by the controller if, in the normal course of events, it is not to be expected that the security breach that has occurred will either still occur or still have a damaging effect;<br>3. individual addressing of the data subjects requires an effort that is unreasonable in relation to the associated costs. In this case, the controller's notification obligation extends to a public announcement or a factually comparable measure.<br><br>**B) Processor**<br>There is a contractual obligation to support the Controller in notifying the data subject of a breach of the protection of their personal data. Corresponding processes to support the Controller in notifying the data subject have been implemented and documented (determination of responsibilities and communication channels).<br>The Processor must assist the Controller, taking into account the nature of the processing and the information available to it, in notifying the data subject of a personal data breach, see Art. 28 para. 3 sentence 2 lit. f GDPR. |

[GDPR] Art. 37, [BDSG] § 38

| | |
|---|---|
| **DP09.03** | **Controller and Processor**<br>If a Data Protection Officer is to be appointed in accordance with Art. 37 para. 1 GDPR, this appointment has been made.<br>In addition to Art. 37 para. 1 lit. b and c GDPR, a Data Protection Officer must be appointed in accordance with Art. 38 para. 1 GDPR, insofar as the Controller or Processor,<br>a) as a rule, employs at least 20 persons who are permanently involved in the automated processing of personal data, or<br>b) carries out processing operations that are subject to a data protection impact assessment pursuant to Art. 35 GDPR (regardless of the number of persons involved in the processing) or<br>they process PD on a commercial basis for the purpose of transmission, anonymised transmission or for the purpose of market or opinion research (regardless of the number of persons involved in the processing). |

| | |
|---|---|
| | • Only persons with appropriate expertise in the field of data protection law and with the ability to fulfil the tasks referred to in Art. 39 (Art. 37para. 5 GDPR) may be appointed as Data Protection Officers.<br>• Contact details of the Data Protection Officer must be published by the controller or processor (Art. 37 para. 7 GDPR).<br>• It must be ensured that the Data Protection Officer is involved properly and at an early stage in all matters relating to the protection of PD (Art. 38 para. 1 GDPR).<br>• The Data Protection Officer may not receive any instructions regarding the fulfilment of his or her tasks (Art. 38 para. 3 sentence 1 GDPR).<br>• The Data Protection Officer must be provided with the resources necessary for the fulfilment of his or her duties (Art. 38 para. 3 sentence 1 GDPR).<br>• The Data Protection Officer reports directly to the highest management level (Art. 38 para. 3 sentence 3 GDPR).<br>• The Data Protection Officer has access to all necessary documentation relating to data protection, data security and information technology.<br>• It is ensured that if the Data Protection Officer fulfils other tasks in the organisation, they are not in a conflict of interest.<br>• There is documentation on the tasks of the Data Protection Officer.<br>• The documentation contains in particular the areas of responsibility listed in Art. 39 GDPR.<br>• The Data Protection Officer has been reported to the competent supervisory authority. |

[GDPR] Art. 24, Art. 38 para. 1 lit. d

| | |
|---|---|
| **DP09.04** | **Controller**<br>A continuous improvement process is in place.<br>• The implemented data protection processes and compliance with legal requirements are reviewed on the basis of the PDCA cycle ('Plan-Do-Check-Act') as part of regular (at least annual) quality and evaluation audits. In this context, the effectiveness of the technical and organisational measures is evaluated and deviations and potential for improvement are identified.<br>• An inspection plan (including inspection methodology) must be created.<br>• Key figures (e.g. individual KPIs) or assessment benchmarks must be defined for the evaluation, which enable the effectiveness of the implemented processes to be assessed and potential for improvement to be identified.<br>• Management review of data protection management system.<br>• Quality and evaluation checks are carried out regularly.<br>• The quality inspection is documented.<br>• A person is appointed to define and update the test criteria for evaluation tests.<br>• A time window is provided within which the proposed measures must be implemented. |

| | |
|---|---|
| | • A specific person is appointed who is responsible for quality and evaluation checks.<br>• The management is informed of the results of the quality and evaluation audits. |

| | |
|---|---|
| DP09.05 | **Controller and Processor**<br>A data protection concept (data protection guideline) is in place that summarises and documents all aspects and processes of the company that are relevant to data protection.<br>The data protection concept (or data protection guideline) is regularly updated (at least annual or or if changes are required) and contains at least the following topics:<br>• Objective and scope of the data protection concept (or data protection guideline)<br>• General data protection policy including the company's data protection objectives<br>• Relevant legal requirements<br>• Responsibilities and data protection organisation<br>• Information on the data protection officer<br>• Reference to principles relating to processing of personal data in accordance with Art. 5 GDPR<br>• Explanations of the need for protection and procedures to determine the need for protection, including risk analysis<br>• Ensuring the rights of data subjects<br>• Handling of personal data breaches<br>• Overview of technical and organisational measures<br>• Maintenance of the record of processing activities<br>• Engagement of processors<br>• Data protection impact assessments<br>• Data protection training<br>• Obligation of employees to maintain confidentiality and data protection<br>• Processes for regular monitoring and review of the data protection organisation<br>• Deletion of data<br>• Sanctions for violations of the data protection concept (or the data protection guideline)<br>• Other applicable documents<br>• Employees must be regularly informed (at least annually and at the beginning of the employment relationship) about the data protection concept (or data protection guideline) and sufficient resources must be available to implement the data protection concept (or data protection guideline). The selection of sufficient resources takes into account personnel capacities and the size of the company.<br>• The employees must have access to the data protection concept (or the data protection guideline) at all times.<br>• There are specific persons responsible for regularly checking that the data protection concept (or data protection guideline) is up to |

| | |
|---|---|
| | date and is updated as necessary.<br>• A change history can be found in the data protection concept (or data protection guideline).<br>• A deadline for checking whether the content is up to date is documented (at least annuall). |

| | |
|---|---|
| DP09.06 | **Controller and Processor**<br>Processes are in place to maintain and regularly review compliance with data protection requirements during ongoing operations. Processes have also been implemented for regular adjustments, particularly in the event of changes to data protection law or IT procedures.<br>The implemented processes take into account at least the following requirements:<br>• Regular reviews (both event-driven and regular) are carried out in the context of data protection.<br>• Appropriate inspection plans are available for regular inspections.<br>• Controllers are defined for carrying out checks in the context of data protection.<br>• The inspection is documented.<br>• A person is appointed to define and update the test criteria for checks in the context of data protection.<br>• A time window is provided within which the proposed measures must be implemented.<br>• Processes are implemented to ensure early and proper involvement of the Data Protection Officer and other relevant bodies (e.g. information/IT security officer) in the event of changes to IT procedures (definition of responsibilities, definition of how and when the Data Protection Officer is to be involved, definition of what information is to be made available to the Data Protection Officer).<br>• Controllers are defined with regard to making any adjustments in the event of changes to data protection law or IT procedures (e.g. adapting the list of processing activities, adapting data protection information and other documents in the context of data protection). |

| | |
|---|---|
| DP09.07 | **Controller and Processor**<br>New or updated software and IT procedures are checked according to a test plan. A test plan must be in place that specifies at least the following:<br>• Roles and responsibilities<br>• Test types to be conducted, test cases and the expected results<br>• Approval criteria<br>• Procedure for situations when approval is refused<br>• Timetable for carrying out the tests including time limit for performing the tests<br>• Resources required to carry out the tests (including hardware, software, personnel)<br>• Test criteria for assessing the quality and completeness of the tests<br>The Data Protection Officer is informed prior to software tests with data that could have a personal reference and a data protection check is carried out prior to the release of IT procedures that process personal data. |

| | |
|---|---|
| DP09.08 | **Controller and Processor**<br>Regular data protection training courses are organised for employees.<br>• A specific person is responsible for organising training courses.<br>• Training documents are available.<br>• The training documents are regularly adapted to current data protection legislation.<br>• The training is mandatory for employees.<br>• Employees are trained in the technical and organisational measures.<br>• Participation in data protection training is documented. |

## DP10 Data protection impact assessment and prior consultation

[GDPR] Art. 35

| | |
|---|---|
| DP10.01 | **A) Controller**<br>If there is an obligation to carry out a data protection impact assessment (DPIA), this will be carried out by the Controller.<br>As part of a threshold analysis, it must first be evaluated whether it is necessary to carry out a DPIA. In this context, it must be determined whether processing, in particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances and purposes of the processing, see Art. 35 para. 1 GDPR.<br>The following test scheme must be implemented:<br>a) Check whether a DPIA must be prepared for processing in accordance with the list of supervisory authorities pursuant to Art. 35 para. 4 GDPR for the (non-)public sector.<br>b) Pursuant to Art. 35 para. 4 GDPR, the supervisory authorities are obliged to draw up a blacklist of processing operations for which a DPIA is to be carried out due to a likely high risk to the rights and freedoms of natural persons. If a processing operation is included in the list, a DPIA must be carried out for this processing operation. If the processing operation is not on the list of supervisory authorities, it must be checked whether a DPIA must be carried out for the processing operation in accordance with Art. 35 para. 3 GDPR. Accordingly, a DPIA must be carried out in the following cases in particular:<br>▪ It is a systematic and comprehensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and which in turn serves as the basis for decisions that have legal effect on natural persons or similarly significantly affect them.<br>▪ This involves extensive processing of special categories of personal data pursuant to Art. 9 para. 1 GDPR<br>c) If the processing operation is also not a case of Art. 35 para. 3 GDPR, it must be examined whether there is nevertheless a high risk pursuant to Art. 35 para. 1 GDPR.<br>When assessing whether the processing is likely to result in a high risk, the guidelines on data protection impact assessment (DPIA) and answering the question of whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679 adopted on 4 April 2017, last revised and adopted on 4 October 2017 (WP 248 Rev. 01) of the Article 29 Working Party, must be taken into account when applying this criterion.<br>The specification of the individual requirements can be found in the test notes.<br><br>Implementation of the DPIA<br>In accordance with Art. 35 para. 7 GDPR, the DPIA must contain at least the following minimum information. The guidelines on a data protection impact assessment (DPIA) and answering the question of whether processing within the meaning of Regulation 2016/679 is "likely to result in a high risk" adopted on 4 April 2017, last revised and adopted on 4 October |

| | |
|---|---|
| | 2017, of the Article 29 Working Party, must be taken into account when applying this criterion.<br>1. systematic description of the planned processing operations and their purposes with the following minimum content<br>▪ Functional description of the processing operations (e.g. processes, IT systems, flow of data, products, interfaces, system boundaries)<br>▪ the nature, scope, circumstances and purposes of the processing must be taken into account (Recital 90 GDPR) (e.g. technology used, such as cloud service, on-premise solution, amount of PD, number of data records, number of parties and service providers involved, circumstances of the processing (automated, paper-based, overt or covert, pseudonymised data or data in plain text)<br>▪ Categories of PD<br>▪ Categories of data subjects<br>▪ Storage duration of the PD<br>▪ Categories of recipients incl. information on possible third country transfers<br>▪ Assets on which PD is based have been identified (hardware, software, networks, people, papers or transmission media for papers)<br>▪ Consideration of compliance with approved codes of conduct pursuant to Art. 40 GDPR (Art. 35 para. 8 GDPR)<br>▪ Specific purposes of the individual data processing operations, including the legal basis for data processing<br>2. where applicable, a description of the legitimate interests pursued by the Controller in connection with the processing<br>▪ where applicable, presentation of the legitimate interests pursued, insofar as the data processing is based on Art. 6 para. 1 lit. f GDPR<br>3. assessment of the necessity and proportionality of the processing in light of its purposes with the following minimum content:<br>▪ measures to comply with the GDPR (Art. 35 para. 7 lit. d GDPR and Recital 90), taking into account the following:<br>a) Measures in terms of proportionality and necessity of processing, on the following basis:<br>○ defined and explicit and legitimate purposes (Art. 5 para. 1 lit. b GDPR) for the processing have been established<br>○ Lawfulness of the processing based on the respective legal basis (Art. 6 GDPR) is given<br>○ Processing operations are adequate, relevant and limited to what is necessary in relation to the purpose (Art. 5 para. 1 lit. c GDPR)<br>○ Limited storage period (Art. 5 para. 1 lit. e GDPR)<br>b) Measures in terms of the rights of the data subjects:<br>○ Information to be provided to the data subjects (Art. 12, 13 and 14 GDPR) is fulfilled<br>○ Data subjects can exercise their rights under Art. 15-21 GDPR without hindrance<br>○ Relationship with Processors (Art. 28 GDPR) is clarified |

| | |
|---|---|
| | ○ Guarantees relating to the international transfer of data (Chapter V of the GDPR) are complied with<br>○ If applicable, prior consultation in accordance with Art. 36 GDPR has taken place<br>4. Assessment of the risks according to cause, type, particularity and severity for the data subjects, taking into account at least<br>○ Identification of sources of risk (Recital 90 GDPR)<br>○ Potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification an disappearance of datathreats that could lead to illegitimate access, undesired modification and disappearance of data are identified<br>○ Assessment of the likelihood and severity of the risks (Recital 90 GDPR)<br>5. Identification of remedial measures to address the risks (Art. 35 para. 7 lit. d GDPR and Recital 90 GDPR).<br>○ Once the risks have been identified, measures to address them must be identified (measures can be technical, organisational or legal)<br>○ At least one appropriate mitigation measure must be taken for each identified risk. If the planned mitigation measures are not sufficient to minimise the residual risks or no mitigation measures can be defined so that the residual risks remain high, the controller must consult the supervisory authority in accordance with Art. 36 GDPR.<br>A DPIA methodology must be selected that meets the criteria set out in Annex 2 of the Guidelines on Data Protection Impact Assessment (DPIA) and on whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679, adopted on 4 April 2017, last revised and adopted on 4 October 2017, of the Article 29 Working Party.<br>A procedural instruction regarding the implementation of a DPIA, including the necessary risk assessment, is in place. This regulates at least:<br>▪ Controller for the implementation of the DPIA<br>▪ Definition of the DPIA process<br>▪ Determination of which information must be provided by the respective specialist department for the DPIA (e.g. using sample forms)<br>▪ Ensure that the DPIA is started as early as possible in the development phase of the processing activities. Appropriate communication channels must be established for this purpose.<br>▪ Regulation regarding obtaining the advice of the Data Protection Officer (when and how)<br>▪ Regulations regarding the consideration of obtaining advice from independent specialists (e.g. lawyers, IT experts, security experts) if required<br>▪ Definition of the DPIA methodology including documentation of the required minimum content<br>▪ Regulation on obtaining the views of the data subjects, or their representatives |

| | |
|---|---|
| | ▪ The roles and responsibilities of the Processor must be contractually defined. The DPIA must be carried out with the support of the Processor, taking into account the nature of the processing and the information available to it (Art. 28 para. 3 lit. f GDPR).<br>▪ Processes for consulting the supervisory authority, see **DP10.04**<br>▪ Determining how the DPIA is to be documented<br>▪ Definitions, including responsibilities, regarding the review of the DPIA and the processing evaluated therein at regular intervals or at the latest when changes have occurred with regard to the risk associated with the processing operations, see **DP10.03.**<br><u>Consultation with affected parties</u><br>In accordance with Art. 35 para. 9 GDPR, the views of the data subjects, or their representatives on the intended processing must be obtained. Controllers, Data subjects, or their representatives must be determined.<br>The opinion can be obtained in various ways depending on the respective context; this must be assessed separately for each individual case.<br>Data subjects or their representatives must be provided with information about the intended processing so that they can make appropriate representations. In particular, the following information must be provided, whereby the provision of information must only take place to the extent that commercial or public interests are not impaired:<br>▪ systematic description of the planned processing operations and their purposes,<br>▪ Where applicable, a description of the Controller's legitimate interests pursued in connection with the processing,<br>▪ Assessment of the necessity and proportionality of the processing against the background of its purposes,<br>▪ Assessment of the risks for the data subjects,<br>▪ Remedial measures to manage the risks.<br>If the Controller's final decision differs from the point of view of the data subjects, the reasons for the further procedure must be documented.<br>If the views of the data subjects are not obtained, the Controller must document why it does not consider such a request to be appropriate.<br>**B) Processor**<br>Taking into account the type of processing and the information available to it, the Processor must support the Controller in carrying out the DPIA (Art. 28 para. 3 lit. f GDPR). For this purpose, especially if the exact mode of operation, risks and protective measures of the IPS are not known to the controller, the necessary information must be kept available in a standardised list or a DPIA must be carried out itself and made available to the controller in each case. |

[GDPR] Art. 35 para. 2

| | |
|---|---|
| DP10.02 | **A) Controller**<br>When carrying out the data protection impact assessment for IPS, the advice of the Data Protection Officer was sought where one was appointed.<br>If the Data Protection Officer's advice is not followed, this must be documented together with the relevant reasons for this.<br><br>**B) Processor**<br>Taking into account the nature of the processing and the information available to it, the Processor must support the Controller in carrying out the DPIA (Art. 28 para. 3 lit. f GDPR). For this purpose, especially if the Controller is not aware of the exact mode of operation, risks and protective measures of the IPS, the necessary information must be provided in a standardised list. |

[GDPR] Art. 35 para. 11

| | |
|---|---|
| DP10.03 | **A) Controller**<br>After the initial data protection impact assessment, the IPS is reviewed on a regular basis (at least annually) or on an ad hoc basis, e.g. in the event of a change in risk, if there is a possibility that previously defined mitigation measures are not followed or the legal or actual framework conditions for processing have changed to ensure that processing is actually carried out in accordance with the identified requirements.<br>Such a review takes place in particular in the event of a change in the risks associated with the processing. The regular review period must be documented.<br><br>**B) Processor**<br>If a standardised list of relevant Information is drawn up, the Processor must regularly check whether the processing is actually carried out in accordance with the identified requirements. Such a review must take place in particular in the event of a change in the risks associated with the processing. If necessary, the standardised list of relevant information must be adapted and the updated version made available to the Controller. |

[GDPR] Art. 36

| | |
|---|---|
| DP10.04 | **A) Controller**<br>If the use of IPS poses a high risk to the rights and freedoms of data subjects and the Controller does not take any measures to mitigate the risk, the Controller must consult the supervisory authority prior to processing. The Controller must provide the following information:<br>1. responsibility of the Controller and Processor involved,<br>2. purposes of the processing,<br>3. means of processing,<br>4. measures and safeguards for the protection of data subjects,<br>5 Contact details of the Data Protection Officer, if applicable,<br>6. The data protection impact assessment.<br>A person must be appointed who is responsible for handling the consultation with the supervisory authority.<br><br>**B) Processor**<br>Taking into account the nature of the processing and the information available to it, the Processor supports the Controller in the prior consultation of the supervisory authority (Art. 28 para. 3 lit. f GDPR). For this purpose, the processor provides the Controller with necessary information to inform the supervisory authority in accordance with Art. 36 (3) GDPR. |

## DP11 Rules of conduct and certification

[GDPR] Art. 40, 41

| | |
|---|---|
| DP11.01 | **Controller and Processor**<br>Where relevant, code of conduct in accordance with Art. 40 GDPR are observed and compliance with them is documented. |

## DP12 Transfer of personal data to third countries or international organisations

**Step 1: Determination of data transfers**

[GDPR] Art. 45 ff.

| | |
|---|---|
| DP12.01 | **Controller and Processor**<br>It must be determined and documented whether and which personal data in the context of the evaluation object (see 1.6) is transferred to which recipients and to which third countries or international organisations. Onward transfers by sub-processors must also be indicated.<br>The transfer of personal data must be appropriate, substantial and limited to what is necessary for the purposes of the transfer.<br>The relevant countries in which personal data is processed, including on behalf of third parties, must be listed. Any onward transfers or extraterritorial access, e.g. due to business activities in third countries, must also be taken into account. The result with regard to the extraterritorial applicability of third country law and any practical extraterritorial application beyond this must be documented.<br>The provider must submit an assessment (e.g. transfer impact assessment) as to whether the Processor and/or the processed data fall under a third country standard or practice that may require unauthorised processing of personal data under European Union law. All circumstances of the individual case must be taken into account and the following points evaluated.<br>a) It is necessary to examine in detail all those legal provisions in which the conditions regarding extraterritorial applicability of third countries' law and, if applicable, practical extraterritorial application go beyond this.<br>b) In the case of extraterritorial applicability and/or application: The result<br>c) The risk that the third country parent company of an EEA subsidiary could instruct it to transfer personal data to a third country.<br>d) It must be evaluated whether the Data Processing Agreement permits unauthorised processing based on third countries' law in accordance with European standards<br>e) any assurances given by the third countries parent company and the EEA company<br>on dealing with conflicting requirements of the law of a third country and European Union law<br>f) an assessment of the legal situation and practice of the third countries as to whether suchAssurances can actually be honoured<br>g) an assessment of all other aspects of whether such assurances are actually honoured<br>h) any data protection breaches identified in the past<br>i) the severity and likelihood of sanctioning infringements under European Union law and the law of the third countries |

| | |
|---|---|
| | j) the exclusion of unauthorised transmissions by means of suitable technical and organisational measures.<br>If a service provider with a branch in the EU, but with a parent company in the USA or in other countries where there is no adequate level of data protection, is used and the storage and processing of all data by the service provider takes place in a data centre within the EU, the personal data must be stored and exchanged in encrypted form in accordance with the state of the art within the meaning of Art. 25 and 32 GDPR and the keys must be managed or stored by the controller in the EU itself (e.g. Customer-Managed Encryption Keys, CMEK, ). A trustee can also take over the management of the keys instead of the Controller, provided that the management of the key takes place in the EU/EEA or in a third country for which an adequacy decision pursuant to Art. 45 GDPR exists.<br>In addition, the respective service provider must guarantee that no data transfer or data processing will be carried out outside the European Union. Both the Controller and its relevant service providers must confirm that no data will be made available in the event of a request for disclosure by the authorities and that no data will be disclosed to the parent company.<br>The specification of the individual requirements can be found in the test notes. |

**Step 2: Documentation of the transmission instruments used**

[GDPR] Art. 45 ff.

| | |
|---|---|
| DP12.02 | **Controller and Processor**<br>If data is transferred to a third country, this transfer is only permitted if one of the following conditions is met:<br>1. The existence of an adequacy decision (Art. 45 GDPR),<br>2. The existence of appropriate safeguards (Art. 46 GDPR),<br>3. The existence of exemptions for certain cases (Art. 49 GDPR).<br>The specification of the individual requirements can be found in the evaluation notes. |

**Step 3: Effectiveness of the transfer instruments in accordance with Art. 46 GDPR**

[GDPR] Art. 46

| | |
|---|---|
| DP12.03 | **Controller and Processor**<br>Appropriate safeguards may include the following:<br>1. a legally binding and enforceable document between public authorities or bodies (Art. 46 para. 2 lit. a GDPR),<br>2. the existence of binding corporate rules (Art. 47 GDPR),<br>3. Standard data protection clauses issued by the EU Commission pursuant to Art. 93 para. 2 GDPR (Art. 46 para. 2 lit. c GDPR),<br>4. Standard data protection clauses adopted by a supervisory authority (Art. 46 para. 2 lit. d GDPR),<br>5. approved codes of conduct pursuant to Art. 40 GDPR together with legally binding and enforceable obligations of the Controller or Processor in the third countries (Art. 46 para. 2 lit. e GDPR), |

| | |
|---|---|
| | 6. an approved certification mechanism pursuant to Art. 42 GDPR together with legally binding and enforceable obligations of the Controller or Processor in the third countries (Art. 46 para. 2 lit. f GDPR).<br>When assessing the effectiveness of the transfer tools in accordance with Art. 46 GDPR, the recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021, and the recommendations 02/2020 on the essential European safeguards in relation to monitoring measures, adopted on 10 November 2020, of the EDPB must be taken into account . The individual evaluation requirements are set out in the following evaluation note.<br>If it is intended to use additional measures that supplement the standard data protection clauses, the approval of the competent supervisory authority for the inclusion of clauses or additional guarantees of such a kind is not required, provided that the additional measures in question do not conflict directly or indirectly with the standard data protection clauses and provided that they offer sufficient assurance that the level of protection guaranteed by the GDPR is not impaired (cf. DP12.04). The data exporter and importer must ensure and be able to demonstrate that the additional clauses cannot be interpreted in a way that limits the rights and obligations set out in the standard data protection clauses or otherwise reduces the level of data protection.<br>If the data exporter intends to amend the standard contractual clauses themselves, or if the additional measures added conflict directly or indirectly with the standard contractual clauses, it can no longer be assumed that the data exporter relies on the standard contractual clauses (SCC); the data exporter must then obtain the approval of the competent supervisory authority in accordance with Art. 46 para. 3 lit. a GDPR.<br>A person must be appointed who is responsible for handling the consultation with the supervisory authority. |

[GDPR] Art. 46 f.

| | |
|---|---|
| DP12.04 | **Controller and Processor**<br>If none of the transfer instruments set out in Art. 46 GDPR are effective, i.e. none of the transfer instruments ensure that the level of protection guaranteed by the GDPR is not undermined by the transfer in practice (see DP12.03), additional measures must be taken to supplement the guarantees under Art. 46 GDPR. These can be of a contractual, technical or organisational nature. Contractual and organisational measures are generally not sufficient, but supplementary technical measures must be implemented.<br>With regard to the selection of effective additional measures, the recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data version 2.0, adopted on 18 June 2021, of the EDPB, must be taken into account when applying this criterion. A list of individual scenarios and the corresponding requirements for technical, organisational and contractual measures is provided in the evaluation note. The corresponding implementation must be explained.<br>The EDPB's 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted |

| | |
|---|---|
| | on June 18, 2021, must be followed as a benchmark for evaluating measures taken to supplement transmission tools (see evaluation note).The specification of the individual requirements can be found in the evaluation notes. |

**Step 5: Reassessment at appropriate intervals**

[GDPR] Art. 46

| | |
|---|---|
| DP12.05 | **Controller and Processor**<br>The Controller and Processor must continuously monitor the situation in the third countries to which they have transferred personal data - where appropriate in cooperation with the service provider - for developments that may be relevant to their initial assessment of the level of protection and the decisions they make regarding its transfers.<br>Appropriate processes must be implemented for this purpose, which at least regulate:<br>• Controller regarding the evaluation of the appropriate level of data protection<br>• Determination of the frequency of the evaluation (at least annually or as required)<br>• Determination of the type and manner of evaluation (cf. requirements for assessing the level of protection in DP12.02)<br>• Involvement of the service provider if necessary (e.g. survey using a sample document)<br>• Suspension or termination of the data transfer if the obligations associated with the transfer instrument pursuant to Art. 46 GDPR are met<br>• Documentation of the evaluation result<br>If it is determined that the obligations pursuant to Art. 46 GDPR have been violated, their fulfilment is impossible or if the additional measures in the third countries concerned are no longer effective, the transfers must be suspended or terminated immediately. Controller and communication channels must be defined for this purpose. |

**Transmission or disclosure not authorised under Union law, Art. 48 GDPR**

[GDPR] Art. 48

| | |
|---|---|
| DP12.06 | **Controller and Processor**<br>Any judgment of a court of a third country and any decision of an administrative authority of a third country requiring a Controller or Processor to transfer or disclose personal data may in any case only be recognised or enforceable if it is based on an international agreement in force, such as a mutual legal assistance treaty between the requesting third country and the EU or Germany, without prejudice to other grounds for transfer under Chapter V GDPR.<br>According to Art. 48 GDPR, official or judicial decisions of third countries as such are not a justifying basis for the transfer of data to a third country. Processes must be implemented and documented for dealing with official or judicial decisions by third countries regarding the transmission and disclosure of personal data.<br>The processes must take the following into account in particular:<br>• Is the request based on a judgement or decision from a court or tribunal or administrative authority of a third country?<br>• Isa the judgement or decision based on an applicable international agreement?<br>• Does the international agreement provide for a legals basis under Article 6 para. 1 lit. c or e GDPR for the transfer of data?<br>• Does the international agreement contain the appropriate safeguards in accordance with Article 42 para. 2 lit. a GDPR and the EDPB Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, version 2.0; adopted on 15 December 2020? |

**Existence of exemptions for certain cases pursuant to Art. 49 GDPR**

[GDPR] Art. 49

| | |
|---|---|
| DP12.07 | Controller and Processor<br>If neither Art. 45 para. 3 GDPR is relevant nor appropriate safeguards according to Art.46 GDPR, including binding corporate rules, exist, a transfer of personal data to a third country or to an international organisation is only permitted under one of the following conditions:<br>a) The data subject has expressly consented to the proposed data transfer after having been informed of the possible risks of such data transfers for them without the existence of an adequacy decision and without appropriate safeguards (Art. 49 para. 1 lit. a GDPR)<br>b) The data transfer is necessary for the performance of a contract between the data subject or for the implementation of pre-contractual measures at the request of the data subject (Art. 49 para. 1 lit. b GDPR)<br>c) The data transfer is necessary for the conclusion or performance of a contract concluded by the Controller and another natural or legal person in the interest of the data subject (Art. 49 para. 1 lit. c GDPR)<br>d) The data transfer takes place for important reasons of public interest (Art. 49 para. 1 lit. d GDPR)<br>e) The data transfer takes place for the assertion, exercise or defence of |

| | |
|---|---|
| | legal claims (Art. 49 para. 1 lit. e GDPR)<br>f) Data is transferred to protect the vital interests of the data subject or other persons if the data subject is physically or legally unable to give their consent (Art. 49 para. 1 lit. f GDPR).<br>g) Data is transferred from a register that is intended for public information in accordance with European Union law or German law , provided that a legitimate interest can be demonstrated (Art. 49 para. 1 lit. g GDPR).<br>Art. 49 GDPR constitutes a derogation. The exemptions under Art. 49 GDPR must therefore be interpreted and applied restrictively. Guidelines 2/2018 on the exemptions under Art. 49 of Regulation 2016/679, adopted on 25 May 2018, must be followed and it must be determined whether the intended transfer actually fulfils the conditions that apply to the individual exemptions. The individual conditions for the exemptions under Art. 49 GDPR are set out in the verification notice and the data exporter must clearly demonstrate the actual fulfilment of the listed conditions. It must be noted that the application of the exemptions must not become the "rule" but is limited to certain situations.<br>The specification of the individual requirements can be found in the evaluation notes. |

# 3. Definitions of terms

The undefined legal terms used in this document are based on their semantic meaning in the context of the GDPR and other normative documents. For a standardised understanding and application of these legal terms, a specific definition is provided below. The individual definitions of terms are based on the description in the Standard Data Protection Model [SDM][4] as well as on publications by data protection supervisory authorities, case law and legal literature.

There is no separate explanation of legal terms that are already defined in the GDPR.

| Term | Description of the |
|---|---|
| **Appropriateness** / **Relevance** / **data** limited to the **necessary extent** ( cf. **DP02.06**) | **Appropriate** data is data that has a specific contextual reference to the Purposes of the processing.<br>**Relevant** data is data whose processing contributes to the fulfilment of the purpose. This characteristic corresponds to suitability in the proportionality test.<br>Only the data that is necessary to achieve the purposes of the processing, i.e. without the processing of which the purposes of the processing cannot be achieved, is **limited to what is necessary.**<br>see [SDM] B1.3 |
| **Anonymise** | Anonymisation is the alteration of personal data in such a way that the details of personal or material circumstances can no longer be attributed to an identified or identifiable natural person or can only be attributed to an identified or identifiable natural person with a disproportionate amount of time, cost and effort, cf. recital 26 GDPR |
| **Basic conception of the evaluation object** | Each evaluation object consists of processing operations that pursue a target function. The application area of the processing operations to be certified is determined by the applicant. |
| **Data minimisation** | Data minimisation covers the basic data protection requirement to limit the processing of personal data to what is adequate, relevant and necessary for the purpose. [SDM C1.1] |
| **Data protection-friendly default settings** | The Controller must take appropriate technical and organisational measures to ensure that, by default, only personal data whose processing is necessary for the specific purposes of the processing is processed. To this end, not only the amount of data processed must be minimised, but also the scope of their processing, their storage period and their accessibility. cf. |
| **Terminal equipment** | A terminal device is any device connected directly or indirectly to the interface of a public telecommunications network for transmitting, processing or recipient of messages; in the case of both direct and indirect connections, the connection can be established via wire, optical fibre or electromagnetically; in the case of an indirect connection, a device is connected between the terminal device and the interface of the public network. |

[4] Standard data protection model, see section 1.5 ("References to laws, regulations and standards").

| | |
|---|---|
| **End user** | An end user is any natural or legal person who utilises a public telecommunications service without themselves providing a public telecommunications network or a publicly accessible telecommunications service. |
| **Freely** | Freely given consent is given if the data subject has a genuine and free choice and is therefore able to refuse or withdraw consent without suffering any disadvantages (i.e. without the risk of deception, intimidation, coercion or other significant adverse consequences (e.g. additional costs) if they do not give their consent. In cases where coercion or pressure is exerted or there is no possibility of exercising free will, consent is not free. |
| **Acting on behalf of** | The Processor or sub-processor serves the interests of another party. |
| **Integrity** | On the one hand, integrity refers to the requirement that information technology processes and systems continuously comply with the specifications that have been defined for them to fulfil their intended functions (B1.6 Integrity). On the other hand, integrity refers to the property that the data to be processed remains intact (B1.6 Integrity), complete, correct and up-to-date (B1.4 Accuracy). Deviations from these properties must be ruled out or at least be detectable (B1.23 Appropriate monitoring of processing) so that they can be taken into account and corrected (B1.22 Remediation and mitigation of data integrity).<br>data breaches).<br>see [SDM] B1.6, C1.3 |
| **Vital interest** | A vital interest is understood to mean an existential interest in the area of health protection, whereby this is not to be equated with "vital". |
| **Delete** | Deletion is the process of making stored personal data unrecognisable. |
| **Accuracy of the data** | The personal data concerned by a processing operation must be accurate and, where necessary, kept up to date. To ensure this requirement, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.<br>*see [SDM] B1.4* |
| **Risk** | A risk within the meaning of the GDPR is the existence of a possibility of the occurrence of an event that itself constitutes harm or may result in harm to natural persons. It has two dimensions: firstly, the severity of the damage and, secondly, the probability that the event and the consequential damage will occur. (see Conference of the Independent Data Protection Supervisory Authorities of the Federal and State Governments, Brief Paper No. 18, p. 1) |

| | |
|---|---|
| **Memory limitation** | Personal data may only be stored in a form which permits the identification of data subjects for as long as is necessary for the purposes for which they are processed. B1.5 "Storage limitation" |
| **Fairness and transparency** | Fairness and transparency in the processing of personal data means ensuring "fair" data processing. This is the case if no unauthorised exercise of rights to the detriment of the data subject is carried out by the Controller and Processor. Furthermore, the principle of fairness and transparency or "fair" data processing requires that the reasonable expectations of the Data subject, must be taken into account. With regard to reasonable expectations, it is necessary to evaluate what the data subject would expect, taking into account the context in which the data are collected, for which their data are processed. An important aspect here is the nature of the relationship between the controller and the data subject, taking into account what is usual and generally to be expected in the given context and in the given (business or other) relationship. The more unexpected or surprising the processing is, the more likely it is to go beyond the reasonable expectations of the data subject |
| Transparency | Data subjects as well as system operators and competent supervisory authorities must be able to recognise to varying degrees which data is collected and processed when and for what purpose in a processing activity, which systems and processes are used for this, where the data flows to and for what purpose, and who has legal responsibility for the data and systems in the various phases of data processing. [SDM] B1.1, C1.6. |
| **Availability** | Availability refers to the requirement that personal data can be accessed and processed immediately and can be used properly in the intended process. To this end, they must be accessible to authorised persons and it must be possible to apply the intended methods for processing them. Availability includes the specific retrievability of data, e.g. through data management systems, structured databases and search functions, and the ability of the technical systems used to make data available to people in an appropriate manner. see [SDM] B1.18, C1.2 |
| **Confidentiality** | Confidentiality refers to the requirement that no unauthorised person can gain knowledge of or use personal data. Unauthorised persons are not only third parties outside the Controller, but also employees of technical service providers who do not need access to personal data to provide the service, or persons in organisational units who have no substantive connection to a processing activity or to the respective data subject. see [SDM] B1.7, C1.4 |
| **Material funds** | Essential means of processing are those that are closely related to the purpose and scope of the processing, in particular the provisions on the type of personal data ("what data is processed"), the duration of the processing ("how long is it processed"), the categories of recipients ("who has access to it") and the categories of data subjects ("whose personal data is processed"). |

| | |
|---|---|
| **Recoverability** | Recoverability is the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident, see [SDM] B1.20. |
| **Purpose limitation** | The obligation to process data only for the purpose for which it was collected can be found in particular in the individual processing authorisations, which make the business purposes, research purposes, etc. the benchmark and is incorporated into the GDPR via the purpose limitation principle in Art. 5 para. 1 lit. c GDPR.<br>Subsequent processing for other purposes must be compatible with the original purpose and take into account the circumstances of the processing (Art. 6 para. 4 GDPR). Data subjects, must be informed of any further processing beyond the original purpose and may exercise their right to object.<br>see [SDM] B1.2 |

# Imprint

Criteria catalogue
for testing the conformity of a
Data processing for the European General Data Protection Regulation


| | |
|---|---|
| Catalogue abbreviation: | **GDPR** |
| Issue: | 2 |
| Version: | 2.16 |
| Stand: | 27.01.2026 |
| Publisher: | TÜVNORD<br>TÜV NORD CERT GmbH<br>Certification authority<br>Am TÜV 1<br>45307 Essen, Germany |
| Editorial office: | **TÜV NORD CERT GmbH** |
| Release: | 03.02.2026 |
| valid until: | Withdrawal |