The Standard Data Protection Model

A method for Data Protection advising
and controlling on the
basis of uniform protection goals

Version 2.0b (english version)

IMPRINT

The Standard Data Protection Model
A method for Data Protection advising and controlling
on the basis of uniform protection goals

Version 2.0b
Adopted by the 99. Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder on the 17. April 2020

Provider:
Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder

Publisher:
AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder

Editor:
UAG „Standard Data Protection Model“ of the AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder

Contact:
Head of the UAG „Standard Data Protection Model“:
Martin Rost
Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein
Holstenstraße 98, 24103 Kiel
E-Mail: uld32@datenschutzzentrum.de
Tel: +49 431 98813 91

Head of the AK Technik:
René Weichelt
Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern
Schloss Schwerin, 19053 Schwerin
E-Mail: rene.weichelt@datenschutz-mv.de
Telefon: +49 385 59494 41

Content

Introduction

The European General Data Protection Regulation (EU) 2016/679)) entered into force on 25. May 2016, and has been deemed valid within the European -Union after a transitional period of two years since the 25. May 2018. The GDPR lays down rules on the protection of natural persons with regard to the processing of personal data and protects the fundamental rights and freedoms of natural persons, in particular their right of protection of personal data. Fundamental requirements on the security of processing personal data are provided in Articles 5, 12, 25 and 32 GDPR. The GDPR calls for appropriate technical and organisational measures to adequately reduce the risks to the rights and freedoms of natural persons. This concerns both measures to safeguard the rights of data subjects (Chapter III GDPR) and measures to implement data protection principles (Art. 25 para. 1 GDPR), including Data Minimisation (Art. 25 para. 2 GDPR) and ensuring the security of processing (Art. 32 para. 1). The principle of data protection by design and by default (Art. 25 GDPR) calls for the controller to address data protection requirements at a very early stage in the planning of processing operations. The GDPR requires a process for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures (Art. 24 para. 1 sentence 2, Art. 32 para. 1 sentence 1 lit. d GDPR). Finally, the GDPR provides a consistency mechanism that integrates the independent supervisory bodies in a complex consultation procedure (Chapter VII GDPR – Cooperation and Consistency). Especially this process requires a coordinated, transparent and verifiable system to assess the processing of personal data with regard to data protection.

Article 5 GDPR drafts basic principles relating to the processing of personal data: Personal data shall be processed lawfully, fairly and in a transparent manner, adequate, relevant and limited to what is necessary for the purpose, on the basis of correct data, protected against loss, destruction or damage and providing for the integrity and confidentiality of such data. In addition, personal data may normally only be stored in a form which permits identification of the data subjects for as long as is necessary. It must be possible to demonstrate compliance with the principles (‘Accountability’).

The Standard Data Protection Model (SDM) provides appropriate measures to transform the regulatory requirements of the GDPR to qualified technical and organisational measures. For this purpose, the SDM first records the legal requirements of the GDPR and then assigns them to the protection goals Data Minimisation, Availability, Integrity, Confidentiality, Transparency, Unlinkability and Intervenability. The SDM thus transposes the legal requirements of the GDPR on protection goals into the technical and organisational measures required by the Regulation, which are described in detail in the SDM's catalogue of reference measures. It thus supports the transformation of abstract legal requirements into concrete technical and organisational measures.

The SDM's catalogue of reference measures can be used to check for each individual processing whether the legally required ‘target’ of measures corresponds to the existing ‘actual’ of measures. The SDM and the catalogue of reference measures also provide a basis for the planning and implementation of the data protection-specific certifications promoted by the GDPR (Art. 42 GDPR) and the data protection impact assessment which is required in certain cases (Art. 35 GDPR).

Such standardisation also supports the cooperation of supervisory authorities, as stipulated in the Regulation. This also entails that the German data protection authorities increasingly cooperate at national level and that their consulting and testing methods must lead to the same data protection assessments. The SDM is created with the aim of providing a coordinated, transparent and verifiable system for data protection assessment.

The SDM can also help implement the National E-Government Strategy (NEGS) adopted by the IT-Planning Council in compliance with data protection regulations. The NEGS calls for technical and organisational measures to ensure data protection which respect the principle of data minimisation and that relate to the protection goals of Availability, Confidentiality, Integrity, Transparency, Unlinkability and Intervenability.

The Standard Data Protection model described here can thus make a significant contribution to the effective and legally compliant implementation of the GDPR in Germany as well as in the international context, both for data protection supervision and for the responsible bodies in the private sector and public administration. The SDM enables a systematic and comprehensible comparison between target specifications, which are derived from standards, contracts, declarations of consent and organisational rules, and the current situation resulting from the implementation of these specifications both at organisational and information technology level in the processing of personal data.

The SDM provides a method for eliminating or at least reducing to a tolerable level the risks to the rights and freedoms of natural persons inherent in the processing of personal data by means of appropriate technical and organisational measures. In addition to such methods and tools, the long-term, individual experiences of the persons acting are indispensable for the creation of data protection and data security concepts. New methods which are comparable to the SDM but are modified in detail result from these experiences and are often used to minimise the risk. These methods can have their merits in specific application contexts.

Part A: Description of the SDM

A1 Purpose of the SDM

The Standard Data Protection Model (SDM) provides a tool to support the selection and evaluation of technical and organisational measures to ensure and demonstrate that personal data are processed in accordance with the requirements of the GDPR. Those measures shall be proportionate and appropriate to limit the risks of the processing to the rights and freedom of the data subjects to such an extent that a level of protection adequate to the risk is ensured. Therefore, it must be examined for each processing whether the personal data are processed by an appropriate selection of technical and organisational measures in such a way that the rights of the data subjects are safeguarded and the security of the processing is guaranteed (Chapter III GDPR and the provisions on security of processing pursuant to Articles 24, 25 and 32 GDPR). The SDM systematises these measures on the basis of protection goals and thus supports the selection of suitable measures. The SDM serves exclusively to design processing activities in compliance with data protection law and does not formulate any requirements that go beyond data protection law.

A prerequisite for the lawfulness of the processing of personal data is the existence of a sufficient and viable legal basis (lawfulness of the processing) and ensuring the security of the data processing. The processing principles pursuant to Art. 5 GDPR and the requirements for the lawfulness of processing pursuant to Art. 6 GDPR shall apply. The validation of the existence of a legal basis as a prerequisite for the admissibility of the processing must take place before the application of the SDM.

The second supposition for the lawfulness of the processing must then be examined cumulatively – the question whether the data processing has been minimised (Art. 25 para. 2 GDPR) and whether appropriate measures have been implemented to reduce the risk to the rights and freedoms of data subjects (Art. 25 para. 1 and 32 para. 1 GDPR). As a first step, this validation presupposes that this risk of processing is clearly identified, as the selection of suitable measures depends on the risks.

In this respect, the SDM is part of an iterative process consisting of the legal evaluation, the design of the processing operations and the selection and implementation of accompanying technical and organisational measures. The SDM and its protection goals offer a transformation aid between law and technology and thus support an ongoing dialogue between participants from the technical, legal and technical-organisational fields. This process runs throughout the entire life cycle of a processing operation and can therefore support the requirement of the GDPR for regular assessment and evaluation of technical and organisational measures, e. g. to ensure the safety of the processing operation (Art. 32 para. 1 lit. d GDPR).

The iterative process described above must start well before the start of processing, at the time when the means for processing are determined (Art. 25 para. 1 GDPR). Already during the first planning stages of a processing activity with personal data, possible risks must be identified and evaluated, in order to be able to assess the consequences of the processing.

In Art. 35, the GDPR obliges the controller with the Data Protection Impact Assessment (DPIA), to assess the necessity and proportionality of processing operations involving particular risks and to carry out a careful analysis, evaluation and planning of the treatment of risks (Art. 35 para. 7 GDPR). The SDM offers a systematic approach for developing a DPIA in a structured form.

The SDM is aimed both at the supervisory authorities and at those responsible for processing personal data. The latter can use the SDM to systematically plan, implement and continuously monitor the necessary functions and technical and organizational measures.

A2 Application scope of the Standard Data Protection Model

The areas of application of the Standard Data Protection model are the planning, implementation and operation of processing activities with which personal data are processed (processing activities with personal data) as well as their validation and assessment. Such processing activities are characterised by the fact that they are directed towards a concrete, delimitable and legally legitimate processing purpose (an enabling provision in the public sector) and towards the business processes that achieve this purpose (see Chapter D2).

The GDPR calls for the selection and implementation of technical and organisational measures for each processing of personal data which are necessary and appropriate according to the state of the art and the risk to the rights and freedoms of natural persons. These measures will be considered as part of the data processing, including any processing of personal data that may be linked to them, and may, where appropriate, become a processing activity of their own. That this is often true in this way is demonstrated by the example of logging, which is usually regarded as a direct component of processing, but must also be assessed from the point of view of employee data protection.

The legal basis may prescribe concrete measures to be implemented in a way specific to the processing, e. g. anonymization of personal data collected once a specific purpose of the processing has been achieved. In addition, there may be cases where specific measures need to be taken as a result of a legal balancing of interests in order to allow processing in conformity with the law.

A3 Structure of the SDM

The Standard Data Protection Model

- systematises data protection requirements in form of protection goals.
- systematically derives generic measures from the protection goals, supplemented by a catalogue of reference measures,

- models the processing activity (business process) with its components data, systems and services as well as subprocesses,
- systematises the identification of risks in order to determine protection requirements of the data subjects resulting from the processing,
- offers a procedure model for modelling, implementation and continuous control and testing of processing activities.

A4 Role of the Protection Goals of the SDM

The SDM uses 'protection goals' to systematise data protection requirements. The data protection requirements aim at legally compliant processing, which must be guaranteed by technical and organisational measures. The guarantee consists in sufficiently reducing the risk of deviations from a legally compliant processing. The deviations to be avoided include unauthorised processing by third parties and the non-implementation of necessary processing operations. The protection goals bundle and structure the data protection requirements and can be operationalised through linked, scalable measures. In this way, the harm to data subjects caused by the processing is minimised and effective protection of data subjects is verifiably ensured by reducing risks to the rights and freedoms of natural persons.

The advantages of working with protection goals are based on the simplified modelling of functional requirements in practical use cases and the simple visualisation of conflicts. The protection goals support the systematic implementation of legal requirements into technical and organisational measures and can therefore be regarded as 'optimisation requirements'.

The SDM specifies seven protection goals of data protection which are of elementary importance for the application of the SDM[1]. In detail, these are:

- Data minimisation
- Availability,
- Integrity;
- Confidentiality;
- Unlinkability,
- Transparency and
- Intervenability.

[1] In order to avoid redundancies, the individual protection goals are not explained in this section of the SDM, but are described in detail in section C1 in connection with their assignment to the legal requirements of the GDPR.

These protection goals reflect the protection objectives in information security that have been tried and tested in practice for many years. The objectives of availability, integrity and confidentiality thus also serve to guarantee information security in public authorities and companies, i. e. to secure and protect the data of an organisation. For experts in the field of information security who are familiar with the Grundschutz concept[2], of the BSI, the German Federal Office for Information Security, protection goals are thus a familiar concept. They will find it easy to use the SDM because the method is based on the IT-Grundschutz and has already proven itself there. Data protection law experts can comprehend the continuity in the development of data protection law and assess the practical benefits of protection goals.

However, data protection does not interpret protection goals from the perspective of the organisation, but from the perspective of the data subjects and encompasses the fulfilment of all data protection requirements for the processing of personal data. The SDM therefore considers the above-mentioned protection goals in their entirety and thus also fulfils the function of combining the known protection objectives of information security and the data protection requirements for the processing of personal data as protection goals.

The concept of protection goals is not new in the context of data protection law. In its key issues paper 'Ein modernes Datenschutzrecht für das 21. Jahrhundert', the Conference of Data Protection Commissioners of the Federal Government and the Länder has published a report on the subject already in March 2010, where they proposed a fundamental reform of the rules of technical and organisational data protection and called for the inclusion of the above-mentioned protection goals in future data protection law[3]. The protection goals had been already embedded in some of the former data protection laws of the Länder.[4] They have therefore been used for many years to implement laws and standards in complex environments with several competing target variables and requirements.

The European legislator has taken up the concept of protection goals in the GDPR and thus pursues the continuous further development of technical data protection from the former control targets of the first Federal Data Protection Act to technology-neutral protection goals. Article 5 GDPR regulates so-called principles of processing, which now claim general validity within the scope of application of the GDPR. Only the fact that these overarching principles have been expressly and universally laid down in the text of the law is new. The central data protection requirements of the General Data Protection Regulation (see Section B2) can be fully systematised by means of protection goals (see Section C). The already known and proven protection goals did not have to be fundamentally changed for this, but their concrete understanding had to be adapted to the General Data Protection regulation.

---

[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[3] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Eckpunkte.pdf

[4] See e. g §§ 4, 5 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) of 9. February 2000 in force until 24. May 2018.

Consequently, it must be stated that all the requirements described in the SDM are completely derived from the GDPR and can be structured with the aid of the protection goals. The SDM does not impose any requirements beyond the applicable data protection law. The protection goals and their concrete understanding will therefore be evaluated and, if necessary, adjusted in the event of future changes to data protection law. The supervisory activities of the data protection supervisory authorities are based exclusively on the GDPR. The SDM's concept of protection goals promotes fundamental rights-oriented data protection and supports controller and data protection supervisory authorities, particularly in systematising the requirements of the GDPR (see Section C2).

Part B: Requirements of the GDPR

The European General Data Protection Regulation (GDPR) applies uniform rules for data protection legislation throughout Europe. The Regulation entered into force on 25 May 2016 and has been directly applicable in all EU Member States since 25 May 2018 pursuant to Art. 99 para. 2 GDPR. Additional regulatory powers have been created for national legislators through numerous supplementary specification clauses. However, the GDPR fundamentally holds precedence over national law. The core of the requirements of the GDPR is laid down in the principles of the processing of personal data in accordance with Art. 5 GDPR, which in turn incorporate the protection task from Art. 8 of the Charter of Fundamental Rights of the European Union.

Accordingly, the GDPR obliges controllers and processors to design the processing operations and the technology used for them with a view to safeguarding the fundamental protection of the rights of the data subjects (Art. 25, 28 GDPR). In order to reduce the resulting risks, including in particular unauthorised access by third parties, the controller is obliged to select the appropriate technical and organisational measures (e. g. Art. 32, 28 para. 3 lit. d GDPR), implement them and check their effectiveness (Art. 32 para. 1 lit. d GDPR). The controller is responsible for compliance with the principles of processing pursuant to Article 5 para 1 and 24 GDPR and must be able to prove their compliance.

The GDPR demands for a data protection impact assessment (DPIA) in accordance with Art. 35 GDPR for processing operations those are likely to pose a high risk to the rights and freedoms of natural persons pursuant to Art. 35 GDPR). The DPIA contains a systematic description of the planned processing operations and specifies technical and organisational measures to overcome the expected risks. This includes safeguards, safety measures and mechanisms which can be used to ensure, verify and evaluate the protection of personal data pursuant to Article 35 para 7 GDPR). The SDM is intended to contribute to implementing the principles for the processing of personal data formulated in Art. 5 of the GDPR and to provide the proof of implementation – with manageable effort – required by the GDPR, e. g. pursuant to Art. 5 para. 2, Art. 24 para. 1 GDPR.

The aim of the SDM is to implement in practice the data protection requirements laid down in the GDPR. Therefore, it is necessary to systematically identify the legal requirements to be met by technical and organisational measures from all the provisions of the GDPR. Firstly, this involves the difficulty that these requirements are scattered throughout the GDPR and have not been grouped together in one place. Secondly, there is the problem that the requirements of the GDPR do not have a uniform degree of concretisation. In some cases, the Regulation already formulates specific requirements such as, in particular, transparency, data minimisation and purpose limitation in Art. 5 para 1 GDPR. In some cases, however, the

legal requirements must first be derived from the rights, obligations and other specifications. An intermediate step from the legal text to the requirement is often necessary, like it has been done with the specification of data protection by default .

The SDM is based on the following data protection requirements, which have been systematically elaborated from the GDPR. The requirements are differentiated into three blocks: key data protection requirements, consent management and implementation of regulatory requirements. The key data protection requirements have to be implemented for every processing of personal data. Consent management summarises the additional requirements to be met if the lawfulness of the processing is based on Art. 6 para. 1 lit. a GDPR. Finally, further requirements may need to be taken into account for the implementation of supervisory measures.

The following passage clearly shows which requirements were derived from which provisions of the GDPR.[5]

The following requirements result directly from Art. 5 para. 1 GDPR:

- Transparency for data subjects affected by the processing of personal data (Art. 5 para. 1 lit. a GDPR),
- Purpose limitation for the processing of personal data (Art. 5 para. 1 lit. b GDPR),
- Data minimisation in the processing of personal data (Art. 5 para. 1 lit. c GDPR),
- Accuracy of personal data (Art. 5 para. 1 lit. d GDPR),
- Storage limitation for personal data (Art. 5 para. 1 lit. e GDPR),
- Integrity of personal data (Art. 5 para. 1 lit. f GDPR, Art. 32 para. 1 lit. b GDPR),
- Confidentiality of personal data (Art. 5 para. 1 lit. f GDPR, Art. 32 para. 1 lit. b GDPR),

The overall requirement is that the controller must be able to demonstrate compliance with paragraph 1.

- Accountability and verifiability (Art. 5 para. 2, Art. 24 para. 1 GDPR).

The GDPR recognises various rights of the data subjects. The rights of the data subjects are explicitly derived from Chapter III of the GDPR (Art. 12-23 GDPR). Pursuant to Art. 12, 24 GDPR, the controller must create the conditions for granting these rights through technical and organisational measures.

---

[5] The SDM does not consider fundamental questions of the substantive lawfulness of a processing operation, nor does it consider special statutory regulations or rules at a high level of detail. Therefore, no requirements that are included in the SDM can be derived from these statutory provisions. The focus on the generally applicable principles of data protection therefore does not spare the obligation to take note of the data protection regulations, not even in the area of technical and organisational measures.

The following individual requirements result from the legal requirement to take into account the rights of data subjects[6]:

- Support in exercising the rights of data subjects (Art. 12 para. 1 and para. 2 GDPR),
- Identification and authentication of the person requesting information (Art. 12 para. 6 GDPR),
- Right to rectification (Art. 16 GDPR),
- Right to erasure (Art. 17 para. 1 GDPR),
- Restriction of data processing (formerly blocking, Art. 18 GDPR),
- Data portability (Art. 20 GDPR)
- Possibility to intervene in processes of automated decisions (Art. 22 para 3 GDPR)
- Freedom from error and discrimination in profiling (Article 22 para 3 and 4, recital 71).

The GDPR strongly promotes data protection through technology. This is already differentiated into several requirements in Art. 25 and 32 GDPR:

- Data Protection by Default (Art. 25 para. 2 GDPR),
- Availability of systems, services and data (Art. 32 para. 1 lit. b and lit. c GDPR),
- Resilience of the systems and services (Art. 32 para. 1 lit. b GDPR),
- Restorability of data and data access (Art. 32 para. 1 lit. c GDPR),
- Evaluability (Art. 32 para. 1 lit. d GDPR).

Controllers pursuant to Articles 33 and 34 of the GDPR have a reporting obligation or, respectively a notification obligation towards the supervisory authorities and those affected by any breaches of the protection of personal data (breaches of data protection). This results in requirements for the proper handling of data breaches. This requires the ability to identify data protection violations (see recital 87 GDPR), classify data protection violations, notify data protection violations to supervisory authorities (Art. 33 GDPR) and notify data subjects of data protection violations (Art. 34 GDPR). This results in the requirements:

- Rectification and mitigation of data protection violations (Art. 33, 34 GDPR)
- adequate monitoring of the processing (Art. 32, 33, 34 GDPR)

If the processing is based on a based on consent , then – in addition to the general requirements – the specific requirements pursuant to Art. 7 and, if applicable, Art. 8 GDPR must be complied with (see B2).

[6]The prerequisites for the rights of data subjects must be validated, but this is not the subject of the SDM.

- Consent management (Art. 4 No. 11, Art. 7 und 8 GDPR).

In Art. 58 GDPR supervisory authorities are granted various powers within the scope of their duties (see Chapter B3):

- Implementation of regulatory orders by a supervisory authority (Art. 58 GDPR)

The order of the following sections is based on the order in which the requirements are formulated in the GDPR.

B1 Key data protection requirements of the GDPR

B1.1 Transparency for data subjects

The principle of Transparency is laid down in Article 5 para 1 lit. a GDPR. It is reflected as a fundamental principle of data protection law in numerous regulations of the GDPR. Especially the information and disclosure obligations pursuant to Art. 12 ff take this principle into account. Art. 12 para. 1 sentence 1 GDPR requires that the controller takes appropriate measures to provide the data subject with all information relating to the information obligations under Art. 13 and 14 GDPR and all notifications pursuant to Art. 15 to 22 and 34 GDPR relating to the processing in a precise, transparent, comprehensible and easily accessible form in clear and simple language. The data subjects must be informed without undue delay and in any case within one month of the status of the processing and of the measures taken with regard to their application pursuant to Art. 12 para. 3 GDPR. The notification obligation pursuant to Art. 34 GDPR in the event of a violation of the protection of personal data, a so-called data breach, also serves the principle of transparency.

B1.2 Purpose limitation

The obligation to process data only for the purpose for which they were collected is particularly evident from the individual processing authorisations, which make business purposes, research purposes etc. the yardstick, and this obligation is incorporated into the Regulation via the principle of Purpose Limitation pursuant to Art. 5 para 1 lit. c GDPR. A subsequent processing for further purposes must be compatible with the original purpose and take into account the circumstances of the processing (Art. 6 para. 4 GDPR). In the case of further processing beyond the original purpose, the data subjects must be informed where applicable, who may then make use of their existing right of objection.

B1.3 Data minimisation

The principle of Data Minimisation is closely linked to the principle of Purpose Limitation. The legislator requires that personal data must be adequate and relevant to the purpose and limited to what is necessary for the purposes of processing (Art. 5 para. 1 lit. c GDPR). This

basic requirement largely corresponds to the basic principle of data economy known from German law. It is only possible to make a limited comparison between the three conditions: appropriate to the purpose, relevant to the purpose and limited to what is necessary for the purposes of processing.

Appropriate data are those that bear a concrete reference to the purpose of the processing, regarding their content. An evaluative decision on the assignment of data and purpose has to be made.

Relevant data are those, whose processing contributes an amount to the achievement of the purpose. This characteristic corresponds to the suitability for the proportionality assessment.

Only those data **are limited to the necessary extent that** are limited to what is necessary for the purpose of processing and without which the processing purpose cannot be achieved. This definition can be derived from recital 39. The processing of personal data is therefore only necessary if the purpose of the processing cannot reasonably be achieved by other means. The encroachment upon the fundamental right to data protection is only permissible if it is limited to the smallest possible extent.

Necessity is a general principle of European Union law which has been recognised and developed by the European Court of Justice (ECJ) over many years. The requirement to process only necessary data is covered in the GDPR by the principle of Data Minimisation (Art. 5 para. 1 lit. b GDPR). It is also required as a prerequisite directly in the licensing provisions pursuant to Art. 6 para. 1 sentence 1 lit. b-f and Art. 9 para. 2 lit. b, c, f-j GDPR.

The principle of Data Minimisation shall be taken into account not only before the start of processing but also on an ongoing basis. For example, the requirement to limit the use to the extent necessary may lead to the requirement to anonymize data at a certain point in time.

The principle of Data Minimisation assumes that the best data protection is achieved when no or as little as possible personal data are processed. The optimisation target is based on the evaluation criterion of minimising the power of authority and knowledge. This principle can be used as an orientation for the optimal series of processing steps, and, as a result, can be adapted to changing conditions. Technical and organisational measures must be taken in the course of processing to ensure that data processing is only carried out within the a priori framework.

The earliest possible erasure of personal data that are no longer needed and thus no longer necessary is one such measure. Even before that, individual data fields or attributes may be excluded from certain forms of processing, or the number of data sets to which functionality is applicable can be restricted. Data fields which enable the identification of the data subjects may be erased or transformed (anonymization, pseudonymisation) or their display suppressed in data masks so that they are not made known to the persons involved in the

processing, provided that this knowledge is unnecessary for the respective processing purpose.

B1.4 Accuracy

Art. 5 para. 1 lit. d GDPR formulates the requirement of the Accuracy of personal data. This means that the personal data concerned by a processing activity must be accurate and, where necessary, kept up to date. In order to ensure that this requirement is met, the Regulation requires that all reasonable steps must be taken to ensure that personal data which are inaccurate with regard to the purposes for which they were processed are erased or rectified without delay.

B1.5 Storage Limitation

The principle of Storage Limitation is defined in Article 5 para. 1 lit. e GDPR in such a way that personal data may only be stored in a form which permits identification of the data subjects for as long as is necessary for the purposes for which they are processed. From this the necessity of measures for pseudonymisation, anonymization or erasures is derived. Furthermore, an exception to this principle is formulated, which is aimed at the processing of personal data exclusively for archival purposes of public interest or for scientific and historical research purposes or for statistical purposes. However, this exception shall apply only subject to the adoption of appropriate technical and organisational measures required by this Regulation to protect the rights and freedoms of the data subject, in particular with a view to enforcing purpose limitation and confidentiality.

B1.6 Integrity

The requirement of Integrity is mentioned in Art. 5 para. 1 lit. f GDPR as a principle for the processing of personal data and in Art. 32 para. 1 lit. b GDPR applied to systems and services as an aspect of safeguarding the security of data processing. It shall ensure, amongst other aspects, protection against unauthorised modifications and deletions. Personal data may only be processed in such a way that ensures protection against accidental loss or destruction or damage by appropriate technical and organisational measures. Any changes to the stored data by unauthorised third parties shall be excluded or at least made recognisable in such a way that they can be rectified.

B1.7 Confidentiality

The obligation to maintain the Confidentiality of personal data results from Art. 5 para. 1 lit. f GDPR. With regard to the systems and services used for processing as well as for the processors and the persons subordinated to the controller or the processor, it results from Art. 32 para. 1 lit. b GDPR. Furthermore, it results from the obligation to follow the instructions of the controller (Art. 29, 32 para. 4 GDPR), a separate obligation of

confidentiality pursuant to Art. 28 para. 3 lit. b GDPR and, if applicable, legal obligations of confidentiality. For data protection officers, it also results from the obligation to maintain secrecy pursuant to Art. 38 para. 5 GDPR. Unauthorised persons must not have access to the data and must not be able to use the data or devices with which they are processed (Art. 32 para. 1 lit. b GDPR, see also Recital 39 sentence 12). A breach of confidentiality is to be assumed in particular if the processing of personal data is carried out without authorisation.

B1.8 Accountability and Verifiability

Art. 5 para. 2 GDPR obliges the controller to prove compliance with the principles on the processing of personal data formulated in Art. 5 para. 1 GDPR. Art. 24 para. 1 sentence 1 GDPR extends this obligation for the controller to the effect that the controller must ensure that the processing is carried out in accordance with this Regulation and must provide proof of this. These comprehensive accountability and verification obligations are substantiated at several points in the GDPR. If the processing of personal data is based on the consent of the data subjects, the controller is obliged pursuant to Art. 7 para. 1 GDPR to be able to prove the consent of the data subjects. In order to verify the processing activities of the controller or processor, Art. 30 GDPR requires the creation of a record of processing activities, in which the individual processing activities are described and the controller must indicate in particular the purpose of each processing activity. In addition, the controller is obliged to document any violation of the protection of personal data for any review by a data protection authority for review purposes pursuant to Art. 33 para. 5 GDPR. The controller must evaluate whether his processing activity is likely to lead to a high risk for the data subjects. In these cases, the controller must be able to prove that he has carried out a data protection impact assessment in accordance with Art. 35 GDPR.

Pursuant to Art. 58 para. 1 lit. a and lit. e GDPR, the supervisory authority may oblige controllers (and processors) to provide all information required for the fulfilment of their tasks upon request. Controllers and processors must be able to fulfil these obligations. The controller must report data breaches to the supervisory authorities under the circumstances regulated in Art. 33 GDPR.

B1.9 Identification and Authentication

Pursuant to Art. 12 para. 6 GDPR, in the event of reasonable doubt the controller may request information from a natural person who wishes to exercise data subjects' rights pursuant to Art. 15 to 21 GDPR, in order to confirm the identity of the data subject. This results in the requirement that the controller must define and implement a process for the authentication of persons who assert the rights of data subjects.

B1.10 Support in the exercise of data subjects' rights

Pursuant to Art. 12 para. 2 GDPR, the controller must facilitate the exercise of the rights of the data subjects pursuant to Art. 15 to 22 GDPR. In any event, applications from data subjects to exercise their rights must be received and examined. Measures to implement the rights of the data subjects must be selected and implemented.

B1.11 Rectification of data

A legal distinction must be made between the principle of the Accuracy of data in Art. 5 para. 1 lit. d GDPR and the possibility of the Rectification of data. This requirement derives directly from the right of the data subject to immediately correct any inaccurate data concerning him or her as laid down in Art. 16 GDPR, a right which may also be claimed by supervisory authorities pursuant to Art. 58 para. 2 lit. g GDPR. Corresponding to this right, the controller has the obligation to carry out the rectification de facto when the requirements are met and to carry out the rectification immediately. Insofar as this cannot be easily achieved, the controller must define suitable procedures (Art. 24, 25 para. 1 in conjunction with Art. 5 para. 1 lit. d GDPR).

B1.12 Erasure of data

Data subjects have the right of Erasure of their data pursuant to Art. 17 para. 1 GDPR, provided that the aforementioned conditions are fulfilled and no exception pursuant to Art. 17 para. 3 GDPR exists. The controller is obliged to erase the data without undue delay. The GDPR does not define erasure. Not the act of erasure but its result is legally decisive. An erasure that is compliant to data protection regulations must result in the data no longer being able to be processed. It must be erased without undue delay.To the extent that this is not readily feasible, the controller must define appropriate policies (Art. 24, 25 para. 1 in conjunction with Art. 5 para. 1 lit. e GDPR). Pursuant to Art. 58 para. 2 lit. g GDPR, supervisory authorities may order the erasure.

B1.13 Restriction of data processing

Art. 18 GDPR provides for the restriction of the processing of data as a supplement to the erasure of data as a data subject's right. Art. 4 No. 3 GDPR defines the restriction of processing as the marking of stored personal data with the aim of limiting their future processing in such a way that they only take place under the conditions specified in Art. 18 para. 2 GDPR (with consent or for the purposes specified therein). The marking must be a technical measure which effectively ensures that the data can only be processed to a limited

extent. Pursuant to Art. 58 para. 2 lit. g GDPR, the supervisory authorities may order the restriction of processing .

B1.14 Data portability

Data portability is a new data subject's right introduced by the GDPR in Art. 20. Pursuant to Art. 20 para. 1 GPDR, the data subject has the right to obtain the respective data in a structured, common and machine-readable format. The provision already sets out specific requirements that have to be fulfilled for the transfer of data sets. Data are considered machine-readable if they are in a file format that is structured in a way that software applications can easily identify, recognise, and extract the concrete data[7]. In addition, the data format must be ‘structured’ and ‘common’. Recital 68 states that the format must be 'interoperable'. The European Data Protection Board states in the Working Paper 242 rev. 01[8] that interoperability should be understood as the objective that can be achieved, inter alia, by means of machine-readable, structured and common data. In order to understand 'interoperability', it refers to Article 2 lit. a of Decision No 922/2009/EC, which defines interoperability as “the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems”.

B1.15 Possibility to intervene in processes of automated decisions

Art. 22 GDPR regulates an additional right of data subjects in relation to automated processing operations – including profiling pursuant to Art. 4 No. 4 GDPR – which lead to legally binding decisions in individual cases. This implies, in certain cases, in accordance with paragraph 3 of this Article, the duty of the controller to take appropriate measures to safeguard the rights and freedoms and the legitimate interests of the data subject, including at least the right to obtain human intervention on the part of the controller , to present his or her views and to contest the decision. The right to intervene presupposes that manual intervention is possible in processes of automated decisions and that a decision can be rectified in individual cases.

B1.16 Freedom from error and discrimination in profiling

Recital 71 specifies the requirements for the processing and evaluation process for profiling in terms of safeguarding the rights and freedoms and the legitimate interests of the data subjects, which are provided for in Art. 22 para. 2 lit. b or a and c of the GDPR in conjunction with Art. 22 para. 3 of the GDPR. Fair and transparent processing must be guaranteed.

---

[7] See recital 21 of Regulation 2013/37/EU.

[8] This working document was originally adopted by EDPB's predecessor institution, the Article 29 Working Party, and later by EDPB with confirmation 1/2018.

Therefore, technical and organisational measures shall be taken for profiling to ensure, in an appropriate manner, that factors leading to inaccurate personal data or to decisions discriminating the data subject are corrected and the risk of error is minimised. As a result, the data processing process should be error-free and non-discriminatory.

B1.17 Data protection by Default

Art. 25 para. 2 GDPR provides for a new data protection obligation for the controller, the implementation of the principle of data protection by default. The controller must take appropriate technical and organisational measures to ensure that by default that only personal data is processed which are necessary for the specific processing purposes. To this end, not only the amount of data processed shall be minimised, but also the extent of its processing, its storage period and its accessibility. Deviations from the default settings can only be made in individual cases in such a way that more comprehensive data processing is carried out or wider accessibility is made possible if the circumstances of these individual cases require a deviation or if the data subject explicitly wishes a deviation. The latter case is of particular importance where the data subject, as a user of an information technology system, can exercise an influence over that system and is given the possibility to choose processing options. If more extensive processing options are available, they may only be switched on and activated by the data subject.

B1.18 Availability

The principle of Availability is enshrined in Art. 5 para. 1 lit. e GDPR and also explicitly included in Art. 32 para. 1 lit. b and c GDPR in the context of the security of data processing. It ensures the availability of the data for the respective purpose as long as this purpose still exists. The principle also applies to the information and disclosure obligations pursuant to Articles 13, 14 and 15 GDPR towards the data subjects. For the implementation of the right to data portability pursuant to Art. 20 GDPR, the requirement of availability is also a basic prerequisite.

B1.19 Resilience

Art. 32 para. 1 lit. b GDPR requires the Resilience of the systems and services. The goal of resilience is not yet known from data protection law, nor is it a classic goal of IT security and is not taken up as a protection goal in the BSI's IT-Grundschutz compendium. It can be taken to mean that the systems and services used for processing will maintain the characteristics necessary to ensure lawful processing even under adverse conditions, in particular those arising from third parties.

B1.20 Recoverability

Art. 32 para. 1 lit. c GDPR demands for the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident in order to ensure the security of processing. These include targeted attacks as well as accidents and unforeseeable events caused, for example, by natural phenomena. The measures to be taken shall focus on the temporal aspect of recoverability. In this respect, the regulation requires in particular process-oriented emergency planning with assigned restart times. In this respect, the recoverability of data and data access goes beyond the general availability required by Art. 32 para. 1 lit. b GDPR. The legislator thus assumes that additional technical and organisational measures must be taken to achieve the objective of rapid recoverability following an incident.

B1.21 Evaluability

The Evaluability demanded for in Art. 32 para. 1 lit. d GDPR does not directly but indirectly serve operational data protection and data security. A process has to be developed and implemented for regular review, assessment and evaluation of the effectiveness of technical and organisational measures to safeguard the security of processing.

B1.22 Remedy and Mitigation of Data Protection Breaches

In accordance with Art. 33 para. 3 lit. d and 34 para. 2 GDPR – in line with Art. 24 and Art. 32 GDPR, the controller must implement technical and organisational measures to remedy the data protection breach and mitigate possible consequences for the data subjects in the event of data protection breaches.

B1.23 Adequate Supervision of Processing

In order to ensure, among other things, effective remedy and mitigation, the controller and the processor may be obliged to monitor the processing in form of a technical and organisational measure within the meaning of Art. 32 GDPR. Moreover, adequate monitoring of the processing can ensure that data protection breaches can be detected and classed immediately within the meaning of recital 87 GDPR.

B2 Consent Management

Consent, as defined in Art. 6 para 1 lit. a in conjunction with Art. 4 No. 11 GDPR, constitutes a special legal basis. If the permissibility of the data processing is to be based on an effective consent, these regulations result in data protection requirements for the consent management, which includes the complete procedure of obtaining, storing, documenting, proving and implementing a withdrawal of consent. In detail, the consent is only effective if

- the data subject has been fully informed of the processing in advance,

- the text of the consent clearly and unambiguously designates specific data processing operations,
- the consent is given voluntarily and
- an unambiguous expression of intention takes the form of a statement or other unclear confirmatory act by which the data subject indicates his or her consent to the processing of personal data concerning him or her.

Finally, it must be possible to withdraw consent at any time with the consequence that the personal data will then no longer be processed, and will be erased in compliance with statutory deadlines.

Art. 7 para. 3 GDPR stipulates that the withdrawal of consent must be as simple as its granting. The controller shall establish appropriate mechanisms for the receipt and implementation of the withdrawal.

In particular, when consent is obtained via electronic means of communication, these legal requirements impose requirements on the design of the process.

B3 Implementation of Supervisory Orders

Art. 58 para. 2 lit. f GDPR allows supervisory authorities to impose restrictions on processing for controllers which may result in the processing not being continued in the intended manner. The restriction may be qualitative or quantitative. For example, qualitative restrictions may include orders that only certain data or data for specific processing purposes may be processed and spatial and temporal processing limits are imposed. One possible quantitative limitation is the limitation of access rights to databases. Restrictions can therefore vary considerably. Due to this diversity, only the rather abstract requirement of the feasibility of supervisory measures can be formulated.

Art. 58 para. 2 lit. j GDPR allows supervisory authorities to order the suspension of the transfer of data to recipients in third countries. The implementation of this order presupposes that the recipients of personal data can be localised and that data transfers can be controlled according to the criteria of the recipient country.

Part C: Systematisation of the Requirements of the GDPR with the use of Protection Goals

The legal standards of the GDPR cannot easily be implemented in technical and organisational terms. Therefore, lawyers and computer scientists must find a common language in the assessment of data protection law in order to ensure that these legal requirements are actually implemented technically and organisationally. They are supported in achieving this target by the protection goals. The requirements (see Part B) are assigned to the individual Protection Goals according to their importance, their intended effect and objective, and are thus structured and bundled. The technical design of processing activities can be based on these objectives, which are geared to feasibility, so that the data protection requirements can be transformed into the required technical and organisational measures via the protection goals.

The aim of the SDM is to make processing activities legally compliant. To this end, it is necessary to implement in practice the data protection requirements laid down by the GDPR and thus to reduce the risks to the rights and freedoms of natural persons as well as to safeguard the security of information processing. The overall objective can only be achieved if several requirements relating to the data – partly alternative, partly cumulative –, systems, services and processes of a processing activity are met by technical and organisational measures. Legal requirements are structured with the help of protection goals. The difference between legal requirements and protection goals lies primarily in the degree of concretisation and systematisation.

C1 Protection Goals of the SDM

The function of the SDM protection goals has already been explained in section A4. Below is a brief description of the protection goals that can be used to systematise the requirements of the GDPR (see Chapter C2).

C1.1 Data Minimisation

The protection goal of Data Minimisation covers the fundamental requirement under data protection law to limit the processing of personal data to what is appropriate, substantial and necessary for the purpose. The implementation of this minimisation requirement has a far-reaching influence on the scope and intensity of the protection concept determined by the other protection goals. Data minimisation specifies and operationalises the principle of necessity in the processing process, which requires of this process as a whole as well as each of its steps not to process more personal data than is needed to achieve the purpose of processing (B1.3 Data minimisation). The minimisation requirement applies not only to the quantity of data processed, but also to the scope of its processing, its storage period and its accessibility. In particular, it is necessary to ensure that personal data are kept in a form which only permits identification of data subjects for as long as is necessary for the purposes

of the processing (B1.5 Storage limitation). Data minimisation starts with the design of the information technology by the manufacturer through its configuration and adaptation to the operating conditions (B1.17 Data Protection by Default) to its use in the core processes of processing as well as in the supporting processes, for example in the maintenance of the systems used.

C1.2 Availability

The protection goal of Availability refers to the requirement that access to personal data and their processing is possible without delay and that the data can be used properly in the intended process. For this purpose, the data must be accessible by authorised parties and the intended methods for processing must be applied to them. Availability includes the concrete retrievability of data, e. g. through data management systems, structured databases and search functions, and the ability of the technical systems used to present data appropriately for humans (B1.18 Availability). Furthermore, measures must be taken to implement availability to ensure that personal data and access to them can be rapidly restored in the event of a physical or technical incident (B1.20 Recoverability). Measures must also be implemented to guarantee the availability of personal data and the systems and services that process them when they are under a reasonable expected load and to ensure that the protection of personal data is not compromised in the event of an unexpectedly high load (B1.19 Resilience). If, in exceptional cases, the protection of personal data with regard to availability is nevertheless violated, it must be ensured that measures are taken to rectify and mitigate the violation (B1.22 Rectification and Mitigation of data protection breaches).

C1.3 Integrity

The protection goal of Integrity refers, on the one hand, to the requirement that information technology processes and systems continuously comply with the specifications that were defined for them to perform their intended functions (B1.6 Integrity). On the other hand, integrity refers to the property that the data to be processed remain intact (B1.6 Integrity), complete, correct and up-to-date (B1.4 Correctness). Deviations from these characteristics must be ruled out or at least detectable (B1.23 Adequate monitoring of processing) so that they can be addressed and corrected (B1.22 Rectification and mitigation of data protection breaches).

This also applies if the underlying systems and services are subject to unexpectedly high loads (B1.19 Resilience). In addition to the aspect of freedom from errors, the aspect of freedom from discrimination must be maintained, especially in automated evaluation and decision-making processes (B1.16 Freedom from errors and discrimination). The factors and characteristics of an assessment or decision-making process that may have potentially discriminatory effects shall be identified a priori in the legal review, and taken into account in implementation and monitored in operation. This aspect is reflected, for example, by measures to clean up training data and validate results when applying AI procedures.

C1.4 Confidentiality

The protection goal of Confidentiality refers to the requirement that no unauthorised person can access or use personal data (B1.7 Confidentiality). Unauthorised persons are not only third parties outside the responsible body, but also employees of technical service providers who do not require access to personal data in order to provide the service, or persons in organisational units who have no connection whatsoever with the content of a processing activity or with the data subject. The confidentiality of personal data must also be ensured when the underlying systems and services are subject to unexpectedly high loads (B1.19 Resilience). Should confidentiality nevertheless be violated in exceptional cases, it must be ensured that measures are taken to remedy and mitigate the accompanying violation of the protection of personal data (B1.22 Remedy and mitigation of data protection violations).

C1.5 Unlinkability

The protection goal of Unlinkability refers to the requirement that personal data shall not be merged, i. e. linked. It must be implemented in practice especially if the data to be merged were collected for different purposes (B1.2 Purpose limitation). The larger and more meaningful the data base, the greater the potential greed may be to use the data beyond the original legal basis. Such further processing is only legally permissible under strictly defined circumstances. The unlinkability is to be ensured by means of technical and organisational measures. In addition to measures for pseudonymisation, other measures that allow further processing separately from the original processing are also suitable, both on the organisation side and on the system side. The data base can be adapted, for example, by authorisation systems and reduction to the extent necessary for the new purpose.

C1.6 Transparency

The protection goal of Transparency refers to the requirement that both data subjects (B1.1 Transparency for data subjects) and system operators (B1.23 Adequate monitoring of processing) and competent supervisory bodies (B1.8 Accountability and verifiability) shall be able to identify to varying degrees which data are collected and processed when and for what purpose in a processing activity, which systems and processes are used to determine where the data are used and for what purpose, and who has legal responsibility for the data and systems in the various phases of data processing. Transparency is necessary for the monitoring and control of data, processes and systems from their creation to their erasure and a prerequisite for legally compliant data processing to which, where necessary, data subjects can give an informed consent (B2 Consent management). Transparency of the whole data processing and of the instances involved can help to ensure that, in particular, data subjects and supervisory bodies can identify deficiencies and, if necessary, demand appropriate changes to the processing.

C1.7 Intervenability

The protection goal of Intervenability refers to the requirement that the data subjects' rights to notification, information, rectification (B1.11 Possibility of rectification of data), erasure (B1.12 Erasure of data), restriction (B1.13 Restriction of processing of data), data portability (B1.14 Data portability), objection and obtaining the intervention in automated individual decisions (B1.15 Possibility of intervention in processes of automated decisions) are granted without undue delay and effectively if the legal requirements exist (B1.10 Support in the exercise of data subjects' rights) and data controller is obliged to implement the corresponding measures. Where the data controller has information enabling him to identify the data subjects, he must also take measures to identify and authenticate the data subjects who wish to exercise their rights (B1.9 Identification and authentication). In order to implement the rights of data subjects and supervisory orders (B3 Implementation of supervisory orders) and to remedy and mitigate data protection breaches (B1.22 Remedying and mitigating data protection breaches), the controllers must at all times be in a position to take action in data processing, from collection to erasure of the data. Where the processing of personal data is based on the consent of the data subject, measures must be taken to ensure that the personal data are processed only where the data subject has given his or her consent and where that consent has not been withdrawn (B2 Consent management).

For information technology processing to which the data subjects themselves have access (e. g. applications on the smartphone) and for which different data protection settings are intended, data-protection friendly default settings must be defined by the controller and further measures must be taken. These further measures must enable data subjects to make their own configurations, differentiated according to the respective processing purposes, and to decide which processing operations they wish to allow that go beyond the minimum required (B1.17 Data protection-friendly default settings).

C2 Structuring the legal requirements with the help of the Protection Goals

In the following table all data protection requirements of the GDPR listed in Section B2 are assigned to the protection goals of the SDM described in Section C2. This assignment serves to systematise the requirements of the GDPR with regard to the technical and organisational design of processing activities, as explained in Section A4.

No.	Requirements of the GDPR	Protection goal
B1.1	Transparency for data subjects (Art. 5 para. 1 lit a, Art. 12 para. 1 and 3 to Art. 15, Art. 34 GDPR)	Transparency
B1.2	Purpose limitation Art. 5 para. 1 lit. c GDPR	Unlinkability
B1.3	Data minimisation (Art. 5 para. 1 lit. c GDPR)	Data Minimisation

No.	Requirements of the GDPR	Protection goal
B1.4	Accuracy (Art. 5 para. 1 lit. d GDPR),	Integrity
B1.5	Storage limitation (Art. 5 para. 1 lit. e GDPR),	Data Minimisation
B1.6	Integrity (Art. 5 para. 1 lit. f GDPR, Art. 32 para. 1 lit. b GDPR),	Integrity
B1.7	Confidentiality (Art. 5 para. 1 lit. f, Art. 28 para. 3 lit. b, Art. 29, Art. 32 para. 1 lit. b, Art. 32 para. 4, Art. 38 para. 5 GDPR),	Confidentiality
B1.8	Accountability and Verifiability (Art. 5 para. 2, Art. 7 para. 1, Art. 24 para. 1, Art. 28 para. 3 lit. a, Art. 30, Art. 33 para. 5, Art. 35, Art. 58 par. 1 lit. a and lit. e GDPR)	Transparency
B1.9	Support in exercising data subjects' rights (Art. 12 para. 2 GDPR)	Intervenability
B1.10	Identification and Authentication (Art. 12 para. 6 GDPR)	Intervenability
B1.11	Rectification of data (Art. 5 lit. d, Art. 16 GDPR)	Intervenability
B1.12	Erasure of Data (Art. 17 para. 1 GDPR)	Intervenability
B1.13	Restriction of data processing (Art. 18 GDPR)	Intervenability
B1.14	Data portability (Art. 20, para 1 GDPR)	Intervenability
B1.15	Possibility to intervene in processes of automated decisions (Art. 22 para 3 GDPR)	Intervenability
B1.16	Freedom from error and discrimination in profilingFehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 para 3, 4 in connection with recital 71)	Integrity
B1.17	Data protection-friendly default settings (Art. 25 para 2 GDPR)	Data Minimisation, Intervenability
B1.18	Availability (Art. 32 para 1 lit. b GDPR)	Availability
B1.19	Resilience (Art. 32 para. 1 lit. b GDPR),	Availability, Integrity, Confidentiality
B1.20	Restorability (Art. 32 para 1 lit. b, lit. c GDPR)	Availability
B1.21	Evaluability (Art. 32 para. 1 lit. d GDPR).	Must be implemented as a process that encompasses all requirements (see Chapter D4 Data Protection Management with SDM).
B1.22	Remedy and mitigation of data protection breaches (Art. 33, para 3 lit. d, Art. 34 para 2 GDPR)	Integrity, Intervenability, Confidentiality, Availability

No.	Requirements of the GDPR	Protection goal
B1.23	Adequate monitoring of the processing (Art. 32, 33, 34 GDPR)	Transparency, Integrity
B2	Consent management (Art. 4 No. 11, Art. 7 and 4 GDPR).	Transparency, Intervenability
B3	Implementation of supervisory orders (Art. 58 para 2 lit. f und lit. j)	Intervenability

Part D: Practical Implementation

D1 Generic Measures

For each of the components to be considered by the SDM (data, systems and services and processes), reference measures are specified and described for each of the protection goals. For each of the measures, the effects on the degree of achievement for other protection goals, which are not directly affected by the measures, shall also be considered. This way, certain individual measures can contribute to the achievement of multiple protection goals.

This section lists generic technical and organisational measures that have been tried and tested in the data protection audit practices of several data protection supervisory authorities for many years. The allocation of these measures to the SDM's protection goals is meant to show that the data protection requirements can be structured in a meaningful way and, as a result, can be systematically implemented. The concrete reference measures can be found in the catalogue of reference measures (in the appendix).

The requirement of the GDPR for evaluability (see Section B1.21) can not be reflected in a protection goal in the SDM, but to be implemented in a cyclical process (data protection management process, see Chapter D4 Data protection management with SDM). It is required that the technical and organisational measures are not only implemented once, but that they have to be evaluated regularly for their effectiveness. In this process, which is to be repeated regularly, it is necessary, for example, to check whether the measures are still appropriate.

D1.1 Availability

Typical measures to guarantee Availability are:

- Creation of backups of data, process states, configurations, data structures, transaction histories, etc. according to a tested concept (B1.20 Recoverability),
- Protection against external influences (malware , sabotage, force majeure) (B1.18 Availability, B1.19 Resilience, B1.22 Rectification and mitigation of data protection violations),
- Documentation of data syntax (B1.18 Availability, B1.20 Recoverability),
- Redundancy of hardware, software and infrastructure (B1.20 availability, B1.19 resilience),
- Implementation of repair strategies and backup processes (B1.19 Resilience, B1.20 Recoverability, B1.22 Rectification and mitigation of data breaches),
- Preparation of an contingency plan for restoring processing activity (B1.19 Resilience, B1.20 Recoverability),
- Representation arrangements for absent employees (B1.18 Availability).

D1.2 Integrity

Typical measures to safeguard integrity or to assess a breach of integrity are:

- Restriction of write and modification permissions (B1.6 Integrity),
- Use of checksums , electronic seals and signatures in accordance with a cryptographic concept (B1.6 Integrity, B1.4 Accuracy, B1.23 Appropriate monitoring of processing, B1.22 Removal and mitigation of data breaches),
- documented assignment of authorisations and roles (B1.6 Integrity),
- erasure or rectifying of incorrect data (B1.4 Accuracy),
- Hardening of IT systems so that they have no or as few secondary functionalities as possible (B1.6 Integrity, B1.19 Resilience),
- Processes for maintaining the timeliness of data (B1.4 Accuracy),
- Processes for identification and authentication of persons and equipment (B1.6 Integrity),
- Definition of the intended behaviour of processes and regular tests to determine and document functionality, risks, security gaps and side effects of processes (B1.6 Integrity, B1.16 Freedom from errors and discrimination in profiling, B1.19 Resilience),
- Determination of the target behaviour of processes and procedures and regular performance of tests to ascertain or determine the current state of processes (B1.6 Integrity, B1.16 Freedom from errors and discrimination in profiling, B1.23 Appropriate monitoring of processing, B1.19 Resilience),
- Protection against external influences (espionage, hacking) (B1.6 Integrity, B1.19 Resilience, B1.22 Rectification and mitigation of data protection violations).

D1.3 Confidentiality

Typical measures to guarantee confidentiality are:

- Definition of an authorisation and role concept according to the necessity principle on the basis of identity management by the controller (B1.7 Confidentiality),
- Implementation of a secure authentication procedure (B1.7 Confidentiality),
- Limitation of authorised personnel to those who are verifiably responsible (locally, professionally), qualified, reliable (if necessary with security clearance) and formally approved, and with whom no conflict of interests may arise in the exercise of their duties (B1.7 Confidentiality),
- Specification and monitoring of the use of authorised resources, in particular communication channels (B1.7 Confidentiality, B1.22 Remedy and mitigation of data breaches),
- specified environments (buildings, rooms) equipped for processing activities (B1.7 Confidentiality),

- Definition and monitoring of organisational processes, internal regulations and contractual obligations (obligation to maintain data secrecy, confidentiality agreements, etc.) (B1.7 Confidentiality, B1.22 Elimination and mitigation of data protection violations),
- Encryption of stored or transferred data and processes for managing and protecting cryptographic information (cryptographic concept) (B1.7 Confidentiality),
- Protection against external influences (espionage, hacking) (B1.7 Confidentiality, Resilience, B1.22 Removal and mitigation of data protection violations).

D1.4 Unlinkability

Typical measures to guarantee unlinkability are:

- Restriction of processing, use and transfer permissions (B1.2 Purpose limitation),
- program-wise omission or deactivation of interfaces in processing methods and components (B1.2 Purpose limitation)
- regulatory measures to prohibit backdoors and quality assurance audits for compliance in software development (B1.2 Purpose limitation),
- Separation according to organisational/departmental boundaries (B1.2 Purpose limitation),
- Separation by means of role concepts with graduated access rights on the basis of identity management by the controler and a secure authentication process (B1.2 Purpose limitation),
- Approval of user-controlled identity management by the controller (B1.2 Purpose limitation),
- Use of purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymised data (B1.2 Purpose limitation),
- regulated processes for amending the purposes of the processing (B1.2 Purpose limitation).

D1.5 Transparency

Typical measures to guarantee transparency are:

- Documentation in the sense of an inventory of all processing activities in accordance with Art. 30 GDPR (B1.8 Accountability and Verifiability),
- Documentation of the components of processing activities, in particular business processes, databases, data flows and network plans, IT systems used for this purpose, operating procedures, descriptions of processing activities, interaction with other processing activities (B1.8 Accountability and verifiability),

- Documentation of tests, of the release and, where appropriate, the data protection impact assessment of new or modified processing activities (B1.8 Accountability and Verifiability),
- Documentation of the factors used for profiling, scoring or semi-automated decisions (B1.8 Accountability and Verifiability),
- Documentation of contracts with internal employees, contracts with external service providers and third parties from whom data is collected or transmitted, business distribution plans, responsibility regulations (B1.8 Accountability and Verifiability),
- Documentation of consents, their revocation and objections (B2 Consent Management),
- Logging of accesses and changes (B1.23 Adequate monitoring of processing, B1.8 Accountability and Verifiability),
- Versioning (B1.23 Appropriate monitoring of processing, B1.8 Accountability and verifiability),
- Documentation of processing by means of protocols on the basis of a logging and evaluation concept (B1.23 Appropriate monitoring of processing, B1.8 Accountability and Verifiability),
- Documentation of the data sources, e. g. the implementation of information duties towards data subjects where their data were collected and the handling of data breaches (B1.1 Transparency for data subjects, B1.8 Accountability and verifiability),
- Notification of data subjects in the event of data breaches or further processing for another purpose (B1.1 Transparency for data subjects),
- Traceability of the activities of the controller for granting data subjects' rights (B1.1 Transparency for data subjects),
- Consideration of the information rights of data subjects in the logging and evaluation concept (B1.1 Transparency for data subjects),
- Provision of information on the processing of personal data to data subjects (B1.1 Transparency for data subjects).

D1.6 Intervenability

Typical measures to guarantee intervenability are:

- Measures for differentiated consent , revocation and objection options (B2 Consent management),
- Creation of necessary data fields, e. g. for blocking indicators, notifications, consents, objections, counterstatements (B1.11 Possibility of correcting data, B1.13 Limitability of processing, B1.17 Data protection through presettings, B2 Consent Management, B3 Implementation of Supervisory Orders),
- documented processing of faults, problem handling and changes to processing activities as well as to technical and organisational measures (B1.22 Rectification and

Mitigation of data protection violations, B1.13 Restriction of processing , B3 Implementation of Supervisory Orders),

- Possibility of deactivating individual functionalities without affecting the overall system (B1.22 Removal and mitigation of data protection violations, B1.13 Limitability of processing, B3 Implementation of supervisory orders),
- Implementation of standardised query and dialogue interfaces for data subjects to assert and/or enforce claims (B1.10 Support in exercising data subjects' rights),
- Operation of an interface for structured, machine-readable data for the retrieval by data subjects (B1.10 Support in exercising data subjects' rights, B1.14 Data portability),
- Identification and authentication of persons who wish to exercise data subjects' rights (B1.9 Identification and authentication),
- Establishment of a Single Point of Contact (SPoC) for data subjects (B1.10 Support in the exercise of data subjects' rights),
- operational possibility of compiling, consistently rectifying, blocking and erasure of all data stored on a person (B1.11 Rectification, B1.12 Erasure, B1.13 Restriction of data processing, B1.14 Data Portability, B3 Implementation of Supervisory Orders),
- Provision of options for data subjects in order to be able to set up programs in line with data protection requirements (B1.10 Support in exercising data subjects' rights, B1.17 Data protection by default).

D1.7 Data Minimisation

The protection goal Data Minimisation can be achieved by:

- Reduction of recorded attributes of data subjects (B1.3 Data Minimisation),
- Reduction of processing options in each processing step (B1.3 Data Minimisation),
- Reduction of the possibility of gaining knowledge of existing data (B1.3 Data Minimisation),
- Establishing default settings for data subjects which limit the processing of their data to what is necessary for the purpose of the processing. (B1.17 Data protection by default),
- Preference for automated processes (not decision processes), which make it unnecessary to gain knowledge of processed data and limit influence in comparison to dialogue controlled processes (B1.3 Data Minimisation),
- Implementation of data masks that suppress data fields, and automatic blocking and erasure routines, pseudonymisation and anonymisation processes (B1.3 Data Minimisation, B1.5 Storage limitation),
- Definition and implementation of an erasure concept (B1.5 Storage limitation),
- Rules for the monitoring of processes to change processing activities (B1.3 Data minimisation).

D1.8 Protection goals as a Design Strategy

The requirements of Art. 25 GDPR must already be taken into account for all levels during the modelling of processing activities. The principle of data protection through technology design ('Data Protection by Design') and data protection-friendly presettings ('Data Protection by Default') formulated in the article require operational data protection requirements to be observed already during the planning phase of a processing operation. Accordingly, technical and organisational measures should not be defined and implemented retrospectively in order to eliminate any non-legally compliant functionalities. Data protection-friendly default settings also require that a specialised application must be configured in order to comply with data protection requirements from the outset. These principles include the principle of data minimisation as a design strategy.

In order to ensure that the functions of the processing activities are designed in a data protection-compliant manner in the sense of 'Data Protection by Design', the protection goals of the SDM can be interpreted as a design principle or design strategy.

For example, the protection goal **Data Minimisation** requires that no more and no other data are collected than those covered by the purpose. Data protection-friendly default settings should result in a default processing of only those personal data whose processing is necessary for the specific purpose for which they are intended. This obligation applies to the quantity of collected personal data, the scope of their processing, their storage period and their accessibility (cf. Art. 25 para 2 GDPR). The protection goals data minimisation and unlinkability can already be realised through the appropriate design of the information technology required for processing. For example, the functional scope of a specialist application must be reduced to the required functions alone. In order to implement the protection goal **Intervenability**, it must be ensured that the rights of the data subjects can actually be implemented by the business application and all other IT services that this application uses, for example at the infrastructure level. This also requires mature change management processes within the organisation. These processes are also necessary in order to respond to changes in the legal framework or to introduce new, more data protection-friendly techniques in existing processing operations. The implementation of the protection goal **Transparency** requires that care must be taken from the outset to ensure that all parties directly or indirectly involved in or affected by processing activities (controllers, processors, data subjects and supervisory authorities) are able to examine the processing activities in accordance with their specific interests.

D2 Processing Activities

The GDPR uses the term 'processing activity' in Art. 30 GDPR as the central concept of data protection management and defines the term 'processing' in Art. 4 para 2 GDPR:

"For the purposes of this Regulation,the term (...)'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;(...)"

Art. 30 GDPR lists the information to be included in the record of processing activities to be carried out by the controller or processor. Among other things, the following are mentioned there

- Names and contact details of the controller, the controller's representative and the data protection officer,
- purposes of the processing,
- a description of the categories of data subjects, personal data and recipients and, where appropriate, the transfer of personal data to a third country or to an international organisation,
- the envisaged time limits for erasure of the data,
- a general description of the technical and organisational security measures referred to in Art. 32 para 1 GDPR.

This general description of a processing does not yet constitute sufficient documentation of processing activities and does not in itself meet the transparency requirements under Art. 5 para 2 GDPR.

The function of the complete documentation of a processing is to make all relevant components of a processing activity verifiable due to the existing accountability, in order to be able to subject these to a data protection evaluation. Verifiability means that the functions of all components used in a processing activity, in particular the components at the level of electronic data processing and communication, are accessible to a target/actual balance sheet.

This test balance regarding functional characteristics as well as the technical and organizational measures taken for the processing activity must then again be subjected to a legal assessment of the legal conformity or regularity as a whole under the aspect of whether the correct measures are selected appropriately and operated with the correct intensity of effect.

D2.1 Levels of a Processing or Processing Activity

In order to fully cover personal data processing, it has proved useful to distinguish at least three different levels of representation of material parameters or elements when designing or auditing processing activities. It is essential to understand that a 'processing activity', for

example, is not congruent with the use of a certain technology or a certain technical program.

Level 1 is the processing of personal data in the sense of data protection law. This processing takes place, for example, within the framework of a company operating under private law or an authority subject to public law, for whose activities the controller is responsible. This level corresponds to what is often understood as a 'specialised procedure' and 'business process' with a certain functional sequence of the processing activity. At this level of the understanding of a processing operation, the personal data necessary for a processing operation as well as the legal requirements are determined. The controller defines corresponding roles and authorisations for the personal data and determines the IT systems and processes to be used. The **determination of the purpose** or purposes of the processing activity is essential for the adequate functioning of this level in terms of data protection.

The practical implementation of the processing and the purpose is located at **level 2**. On the one hand, this usually includes the role of the clerking as well as the IT application(s), which can also be described more precisely as the 'specialised application of a specialist procedure'. The processing and the specialist application must completely fulfil the functional and (data protection) legal requirements to which the processing is subject. **The specialised application must ensure the purpose limitation.** The application must exclude the processing of additional data or additional forms of processing, even if they may be functionally particularly convenient. The aim is to minimise the risk of undermining the purpose limitation or overstretching the purpose.

Level 3 houses the IT infrastructure that provides functions that are used by a level 2 application. This level of 'technical services' includes operating systems, virtual systems, databases, authentication and authorisation systems, routers and firewalls, storage systems such as SAN or NAS, CPU clusters, and the communications infrastructure of an organization such as the telephone, LAN, or Internet access. These systems must be designed and used within a processing activity in such a way that the **purpose limitation** is retained. Typically, technical and organisational measures must be taken to ensure that the purpose limitation or segregation of purposes can be enforced at this level.

D2.2 Purpose

Prior to the application of the SDM it must be clarified whether a processing operation follows a legitimate purpose and whether the purpose of the processing operation is sufficiently determined (see Section D4.2).

When implementing the specific purpose of a processing operation, it has proved successful to consider two further aspects in order to also achieve a sufficient purpose limitation of the processing activity:

- In addition to the intended purpose, the aspects of **purpose differentiation** or **separation of purposes** must also be considered. It should be specified which

(related) purposes should not be implemented by the processing activity in question. This facilitates a legally compliant separation of the processing activities among each other as well as the separation of data sets, systems and services as well as processes on the IT level in particular.

- The aspect of **purpose limitation** must also be taken into account. The purpose limitation of a processing operation must be ensured on the one hand by its suitable functionality and by suitable selection of the production or user data to be processed (horizontal design). However, the purpose limitation of a processing operation must also be ensured by a suitable cross-level design (see Section D2.1) (vertical design). For example it is usually not covered by the purpose and operationally also not necessary that beside the authorised clerks and their superiors also IT administrators, who administer the access rights for example on the level of a data base, can gain knowledge of the contents of the processing data.

D2.3 Components of processing or processing activity

The data, systems and services components result directly from the requirements of the GDPR. However, it is necessary to consider the following three components when modeling processing activities with reference to persons:

1. personal **data**
2. the technical **systems and services** involved (hardware, microservices, software and infrastructure) ,
3. the technical, organisational and personnel **processes** involved in processing data.

The term 'process' is not explicitly included in the GDPR. Each processing activity can be modeled as a business process or technical procedure and consists of individual processing steps. Individual processing operations are, for example, collection, recording, sorting or storage until erasure or destruction (cf. Art. 4 No. 2 GDPR). These processes are modeled or implemented as subprocesses.

In methodological terms, the first priority is the personal data whose need for processing must be measured in advance in relation to the intended purpose.

The concrete functional design takes place at level 1, at which the need for protection is to be determined or specified by the controller on the basis of the data. This need for protection is inherited by all data, systems and processes used in concrete processing at the various levels. The catalogue of reference measures can be used to check whether technical and organisational measures taken or planned are appropriate to the need for protection.

With these three core components data, systems and services as well as processes, the following special properties, among others, also play an important role:

It is necessary to look at the properties of ***data formats*** that are used to collect and process data. Data formats may have an influence on the quality of the implementation of the

protection goals, e. g. where it can not be considered sufficiently clear what data is contained in files with certain formats. For example, text files may contain data that is supposedly deleted and does not appear in the printout; graphic files may contain metadata such as camera model, location and time of recording, or relevant information may fall victim to compression in graphic, video and audio files.

For the systems involved, it is necessary to consider the interfaces that a specialised application has with IT systems on level 3, as well as those it has with other systems that are not within the system boundary defined by the purpose. In addition to these vertical interfaces, horizontal interfaces must also be taken into account, which entail a risk for purpose limitation. The documentation of the existence of interfaces as well as the documentation of their properties are of decisive importance for the legal responsibility, controllability and verifiability of data flows.

For each processing activity and its components, in particular for the sometimes difficult to grasp processes across different systems, the **controllership** must be clarified and documented in the list of processing activities pursuant to Art. 30 GDPR. According to Art. 4 para. 7 GDPR, a controller is "(...) the natural or legal person, public authority, agency or other body (...) which, alone or jointly with others, determines the purposes and means of the processing of personal data; (...)". Tasks resulting from controllership may be delegated in the form of individual responsibilities. These responsibilities are typically formulated and assigned as roles in a comprehensive authorisation and role concept. The responsibility of a process owner can extend to individual processes (subprocesses) or to the entire processing activity across all process levels in the sense of overall responsibility. This responsibility can be distributed among different roles, each with partial responsibilities. If the processing activity involves a processor according to Art. 28 GDPR, it must be ensured that the processor fulfils his tasks in accordance with the instructions of the data protection controller.

Ultimately, the responsibility for the processing always lies with the controller within the meaning of Art. 4 para. 7 GDPR.

D3 Risks and Need for Protection

The GDPR links the requirements for technical and organisational measures to the risk associated with the processing of personal data for the rights and freedoms of data subjects.

The short paper No. 18 "Risiken für die Rechte und Freiheiten natürlicher Personen (Risks to the rights and freedoms of natural persons)"[9] of the Data Protection Conference explains the concept of risk in the context of the GDPR and shows in general terms how risks to the rights

[9] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, As of: 26.04.2018, last retrieved: 29.07.2019.

and freedoms of natural persons can be identified and assessed in relation to their legal consequences.

A risk within the meaning of the GDPR is the possibility of the occurrence of an event which may damage the rights and freedoms of natural persons (including unjustified impairment of rights and freedoms) or result in harm to one or more natural persons. It has two dimensions: Firstly, the severity of the damage to the rights and freedoms of the data subjects and, secondly, the probability that the event and the damage will occur.

According to recital 75, possible damage to the rights and freedoms of natural persons includes physical, material and immaterial damage. In the following, we will generally speak of damaging events. A damaging event can damage or impair various rights and freedoms and possibly result in further damaging events. Unlawful processing activities, in particular those which do not comply with the principles of Art. 5 GDPR, are in themselves impairments of the fundamental right to data protection and therefore already constitute a damaging event. They can cause additional damage, such as discrimination against natural persons[10].

The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, extent, circumstances and purposes of the processing.

The task of the controller is to identify, analyse and categorize these risks and to take measures to contain them (see Chapter D4 Data protection management with the SDM).

This Chapter D3 provides guidance to determine the data protection risk of a processing activity. It also establishes the connection between the risks posed by a processing activity and protection requirements of natural persons with regard to the processing of personal data caused by it (Art. 1 para. 1 GDPR) on the one hand and the level of protection achieved by the implemented measures or the residual risk of a processing activity on the other, with the aim of enabling the determination of suitable and appropriate measures. Determining the level of risk is the prerequisite for being able to define technical and organisational measures and the necessary degree of their effectiveness with which risks can be eliminated or at least reduced and processing can take place in compliance with data protection requirements. As a general rule, the higher the risk, the more prudent the processing activity must be and the more effective the specific technical and organisational measures must be operated, monitored and, if necessary, improved.

D3.1 Risks for Data Subjects

The starting point for risk considerations is the processing activity , which consists of one or more processing operations. The term ‘processing activity’ introduced in Art. 30 GDPR is

[10] This definition of risk can be derived from recital 75 GDPR.

used, because according to the definition in Art. 4 No. 2 GDPR, processing means any or set of operations. Any processing activity must comply with the principles on the processing of personal data set out in Art. 5 GDPR. The SDM 'consolidates' these principles into protection goals that incorporate further operational requirements of the GDPR. In principle, any processing activity creates risks for data subjects due to the fact of processing personal data.

In contrast to general risk management and risk management in information security, there is a fundamental obligation in the area of data protection to reduce the risks arising from the processing of personal data to an appropriate level of protection with appropriate technical and organisational measures. According to the GDPR, it is not permissible to completely dispense with the handling of requirements, in particular the implementation of the principles of Art. 5 GDPR, and to accept the resulting risks. The instruments of risk acceptance or risk transfer known from the field of information security are not available to the controller in the context of data protection. There is scope in the selection and manner of implementing requirements by means of technical and organisational measures which are required to an appropriate extent (Art. 5 para. 1 lit. d 'reasonable steps', (f) 'appropriate security'). It is necessary to analyse existing risks to the rights and freedoms of natural persons in more detail. Only when an adequate level of protection has been achieved and the interests of the data subjects have been adequately taken into account can the remaining residual risks be accepted by the Controller.

Art. 35 GDPR requires the controller to carry out a data protection impact assessment for the intended processing in the event of a 'likely high risk' for the rights and freedoms of natural persons. In order to determine the level of risk, the controller must therefore first carry out a 'threshold analysis '. This analysis must be carried out for each processing activity, consisting of one or more processing operations, in order to be able to justify the decision the classification of a processing activity to a competent data protection supervisory authority (accountability pursuant to Art. 5 para. 2 GDPR) .

If the result of the threshold analysis shows an 'likely high risk to the rights and freedoms of natural persons', this must have an impact on the design of the processing activity and its verifiability.

The central methodological question for the design of a processing activity is therefore how to determine the level of risk for a processing activity.

D3.2 Risk Assessment

D3.2.1 Threshold analysis

The aim of the threshold analysis is to determine whether a processing activity is likely to pose a high risk to the rights and freedoms of natural persons and thus require a DPIA. In order to identify a possible 'high risk' from a processing activity, the following procedure is proposed, which does not necessarily have to be followed in order:

A. Check whether the processing activity for which the risk has to be determined is included in the 'mandatory list' of the data protection supervisory authorities pursuant to Art. 35 para. 4 GDPR. If so, the risk is likely high. (For the private sector are https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf, as of October 17th, 2018, last access: April 1st, 2019).

B. Examine whether the processing activity under consideration is one of the particularly risky processing activities pursuant to Art. 35 para. 3 GDPR. If this is the case, the risk is likely high.

C. Check whether the processing activity is subject to characteristics contained in the list of processing activities 'likely to be high-risk' of Working Paper 248 rev. 01[11] of the European Data Protection Committee. If at least two of the entries apply, it should be assumed in most cases that there is likely to be a high risk. However, a high risk may also exist if only one of the criteria is fulfilled.

1. Evaluation or scoring, including profiling and predicting, especially from "*aspects concerning the data subject's performance at work*, *economic situation*, *health*, *personal preferences or interests*, *reliability or behavior*, *location or movements*" (recitals 71 and 91).
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person" or which "similarly significantly affects the natural person*" (Article 35(3)(a)).
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))
4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10.
5. Data processed on a large scale.
6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
7. Data concerning vulnerable data subjects (recital 75).
8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.

[11] This working paper was originally adopted by the EDPB's predecessor institution, the Article 29 Working Party, and later by the EDPA with confirmation 1/2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, status: 13.10.2017 (Revision 0.1; last access: 01.04.2019)

9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (Article 22 and recital 91).

   (from: WP 248 of the Art. 29 Working Party, from page 10 f)

4. Check whether the nature, scope, circumstances or purposes (recital 76 GDPR) of the processing activity increase the risk to data subjects. To this end, it is advisable to include appropriate practical experience and concrete court rulings in the examination of a possibly existing high risk.

D3.2.2 Risk Identification

In order to identify concrete risks to the rights and freedoms of data subjects, which may also arise from specific characteristics of the processing activity, it is appropriate to ask the following questions:

a) What damage may occur to data subjects on the basis of the data to be processed?
b) What events can cause the damage?
c) By what actions and circumstances may these events occur?

This step in particular may, in exceptional cases, identify risks that could lead to very serious consequences for the persons concerned, such as a danger to life and limb. In such cases, it makes sense to assume a very high protection requirement (see Section D3.3). However, the technical and organisational measures proposed by the SDM are not designed for this purpose, meaning that in such a case, as it is also the case for high protection requirements, an individual consideration of the possible measures must always be carried out in order to establish an appropriate level of protection. However, the measures of the SDM can serve as a starting point for this individual consideration.

In addition to the specific data protection risks of a processing activity itself, the risks of information security must also be considered. These risks relate to the protection of the organisation's business processes. The BSI's IT-Grundschutz has proven its worth in dealing with these risks (https://www.bsi.de). Essential aspects of basic protection measures (Grundschutz) include orderly operation, ensuring the availability and integrity of data, systems and services, and preventing unauthorised access to business, production and personal data, i. e. ensuring confidentiality. These are also prerequisites for effective data protection. It is very important to ensure that, when coordinating measures for information security and operational data protection, in particular those protective measures which are operated for IT security are themselves set up in compliance with data protection regulations (e. g. video surveillance for securing properties, cloud solutions for malware protection or logging). Any conflicts between the requirements of data protection and information security must be resolved.

D3.2.3 Risk Assessment

It is the responsibility of the controller and, if necessary, of the processor to analyse and categorize the risks identified for the data subjects. The controller or the processor must determine and document the severity and probability of occurrence of the identified risks according to objective standards. Based on this assessment and on the basis of a risk function (e. g. in the form of a risk matrix), the respective level of risk is determined (cf. short paper No. 18 "Risiko für die Rechte und Freiheiten natürlicher Personen"(Risks to the rights and freedoms of natural persons)[12]).

D3.3 Level of risk, level of required protection , level of protection and residual risk

The need for protection of the rights and freedoms of a natural person with regard to the processing of personal data derives from the risk posed by the processing activity and its intensity of intervention. The GDPR only knows the terms 'risk' and 'high risk', whereby 'risk' is here referred to as 'normal risk'. In addition, the GDPR uses the wording 'unlikely to result in a risk' (Art. 27 para. 2 lit. a and Art. 33 para. 1 GDPR). Since there can be no completely risk-free processing, the phrase 'not leading to a risk' is understood from its meaning and purpose as leading to 'only to a low risk'. Practical experience shows that there are such low risks which are not mentioned separately in the GDPR, but for which measures must also be taken. The measures for the normal need for protection also cover such low risks.

The need for protection arises from the risk of the processing activity before technical and organisational measures have been determined and implemented. In this respect, the following relationship applies between risk (level), in the sense of an initial risk, and protection requirements (level) :

- **no or little risk** of the processing
  -> normal need for protection for data subjects
- **normal risk** of the processing
  -> normal need for protection for data subjects
- **high risk** of the processing
  -> high need for protection of data subjects

While the protection requirements of data subjects with regard to processing activities defined by the initial risk remain constant, the processing risks for the data subjects can be reduced by technical and organizational measures. These measures do not change protection requirements, but reduce the risk of processing activities. The risks initially present – the initial risks – must be reduced by process design and technical and organisational measures until a level of protection appropriate to the risk (Art. 32 para. 1

[12] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, As of: 26. April 2018, last access: 01. April 2019.

GDPR) for the processing activity is guaranteed. In other words, the level of protection must be high enough to ensure that the controller can prove that the remaining residual risks of a processing operation can be justified. If there is no reasonable residual risk, the processing activity may not be commenced due to lack of legal conformity. If a risk at “high” or beyond is remaining Art. 36 GDPR stipulates that the controller shall consult the competent data protection supervisory authority.

The BSI's IT-Grundschutz methodology also uses the concept of protection requirement categories to ensure information security in order to scale the effects of technical and organisational measures.

Due to the different aims of BSI's IT-Grundschutz (safeguarding the information security of an organisation) and ‘operational data protection’ with the help of the SDM (safeguarding the rights and freedoms of natural persons), it cannot be ruled out that the findings on the need for protection under Grundschutz and SDM for the same processing may be different. In the event of different assessments, either the respective measures for the higher protection needs should be implemented or a more detailed analysis should be carried out to identify the reason for the different assessments and how an adequate level of protection can be achieved in this case. The data protection requirements are decisive. These analysis and decision-making processes with their associated assessment shall be documented. Both, during an internal company or organisation evaluation or revision or during a data protection audit, it must be possible to trace which concrete technical and organisational measures have been taken to achieve the required level of protection with regard to the respective processing activity.

D3.4 Determination of technical and organisational measures, especially in the case of high risk

In principle, data processing processes and thus the specification of data processing are to be designed in such a way that, if possible, processing is carried out without reference to persons or at least the risks are reduced If, for example, it has been identified that automated retrieval procedures pose high risks to the rights and freedoms of natural persons because unnecessary retrievals cannot be technically prevented or the data volume of retrievals cannot be adequately restricted by the person retrieving the data, there is a further possibility to limit the risk by waiving the automated retrieval procedure and implementing a transmission for individual cases as an alternative.

When appropriate technical and organisational measures are taken, the state of the art shall be taken into account. The technical and organisational measures proposed in section D1 ‘Generic measures’ provide a good basis for developing adequate measures for normal protection needs. In the future, these generic measures will be supplemented by the catalogue of reference measures. In the case of a high or very high need for protection, the following standardised strategy for effective risk reduction is recommended.

1. The measures in the catalogue of reference measures to be taken in the event of normal initial risk or need for protection shall be implemented.
2. Additional measures from the catalogue of reference measures must be implemented.
3. Individual measures must also be selected.
   An example of an individual measure could be the approval of certain operations of a processing activity only on request or after an audit, and then to monitor that activity in the enterprise so that a termination or corrective action is triggered in case of deviations.
4. The effect of a measure can be increased by using scaling possibilities.
   An example would be the increase of the length of cryptographic keys used. Another example would be the backup of log data by operating a dedicated log server for the processing of log data, which stores all log data in a central location and removes the log data from the access in production machines and by their administrators.
5. Technical and organisational measures shall be applied to all measures already taken in order to improve the effectiveness, reliability, robustness, resilience and evaluability of the measures and to ensure their legality.
   The following example illustrates the strategy of self-application of the measures to themselves. Transparency means that a processing activity must be verifiable on the basis of target/actual balances. Retrospectivity means that log data must be generated, stored and processed. The log data must then be stored in a revision-proof manner by applying additional measures and their confidentiality must safeguarded by being signed and transmitted and stored in an encrypted way.

It should be noted that new risks may arise as a result of technical and organisational measures taken. These risks must be assessed and appropriately reduced. As an example, a full logging of employee actions can be required, which at the same time harbours the risk that an inadmissible monitoring of performance and behaviour takes place through evaluations of this log. If a processing is modified during this step in such a way that the measures taken lead to new risks that are higher than the initial risk and thus lead to an increase in the need for protection, the design of the measures must be re-evaluated. The above mentioned strategies shall be applied in an iterative process until the design of the measures ensures an adequate level of protection.

D4 Data Protection Management with the Standard Data Protection Model

Data protection management is a comprehensive method for systematically implementing all the requirements of data protection law in an organisation. In the following, a data protection management in interaction with the SDM is described in more detail.

D4.1 Legal Basis for Data Protection Management

The controller is responsible for compliance with the principles governing the processing of personal data and must be able to provide evidence of such compliance. Specifically, the controller must, pursuant to Art. 30 GDPR, keep a catalogue with the processing activities of personal data by the organisations. In addition, he must already take appropriate technical and organisational measures at the time the means are determined (Art. 25 para. 1 GDPR - Data protection by design). For processing activities which are likely to result in a high risk for the rights and freedoms of natural persons, he must also carry out a data protection impact assessment (DPIA) in accordance with Art. 35 GDPR. In order to assess whether a processing activity is likely to pose a high risk and therefore require the carrying out of a DPIA, a threshold analysis must be carried out for each processing operation. Even without a DPIA, appropriate technical and organisational measures must be identified and permanently implemented to ensure a level of protection appropriate to the risk involved in any processing of personal data. Finally, the controller must be able to demonstrate, evaluate and, if necessary, improve the implementation and effectiveness of the measures and in this way keep them up to date.

In order for the controller to be able to comply with the detailed requirements relating to the operational implementation of the data subjects' rights and his accountability and verification obligations (cf. Section B1.8), a systematic approach is required in the audit and assessment, which relates both to each individual processing activity and to all processing activities relating to individuals within the entire organisation and the associated technical and organisational measures. These accountability and verification obligations are a ongoing task for the controller and should therefore be established as a ongoing cyclical process. The proven PDCA cycle (Plan, Do, Check, Act), which is familiar from quality management, provides a continuous improvement process in four phases, which forms the basis for the data protection management process (DPM process) described here.

The DPM process thus serves on the one hand the controller for the systematic planning, the permanent operation, for the regular checking of data protection conformity and the improvement of processing activities (cf. B1.21 Evaluability). It thus creates transparency for the controller. On the other hand, the DPM process also assists data protection supervisory authorities in advising data controllers and in the data protection audit of these processing activities, as the data protection audits of the supervisory authorities generally correspond to this process flow.

D4.2 Preparations

Before starting the DPM cycle and before using the SDM[13], the following three prerequisites must be clarified:

[13] see Fn. 5.

1. Clarity about the factual circumstances in which the data processing to be considered takes place or is to take place.
2. Validation of the lawfulness of the processing. [14]
3. Further substantive assessments of the lawfulness of this processing.

In order to determine the factual circumstances at the controller of the processing activity, the following questions, for example, must be clarified:

- Which bodies are involved in the processing?
- Who is responsible for which parts of the processing?
- Which business processes of the controller are supported by the processing?
- Which data are processed in which steps and using which systems and networks?
- Which persons carry out the data processing and which persons carry out the monitoring?
- Which auxiliary processes are used to support the processing activity?

In the context of the validation of the lawfulness of the processing, the legal basis for the processing must be determined. In particular, the following questions derived from Art. 6 para. 1 GDPR may be used for this purpose when processing personal data[15]:

- Does the consent of the data subjects constitute the legal basis for the processing activity?
- Is the processing necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request of the data subject?
- Is the processing necessary to fulfil a legal obligation to which the controller is subject?
- Is the processing necessary to protect the vital interests of the data subject or of another natural person?
- Is the processing necessary for the performance of a task carried out in the public interest or in the exercise of official powers vested in the controller?
- Is the processing necessary to safeguard the legitimate interests of the controller or of a third party? Do the interests or fundamental rights and freedoms of the data subject which require the protection of their personal data prevail, in particular where the data subject is a child?

The substantive evaluation assesses the extent to which the processing activity planned by the data controller and, if applicable, the activity to be audited by the supervisory authority is fundamentally permissible. In addition, it provides answers, in particular, to the following questions which prepare the application of the SDM:

[14] For the differentiation between admissibility and lawfulness see Chapter A1.

[15] If special categories of personal data are processed, Art. 9 GDPR must also be observed.

- Which national law is applicable to the processing?
- What legitimate purposes can be legitimately pursued with the processing and what changes of purpose in the course of processing are permissible?
- What data are substantial and necessary in order to achieve the permitted purposes?
- What are the legal bases for the transfer of data to persons within and outside the participating bodies and from these to third parties?
- Have the necessary agreements been made if several controllers are involved in the processing activity and are jointly responsible (Art. 26 GDPR)?
- Are processors involved in the processing and are the legal relationships between them defined (Art. 28 GDPR)?
- What special requirements must the technical and organisational measures meet in each individual case?

The level of detail, especially of the findings on the factual circumstances, will vary from processing to processing, as will the degree of formalisation of the procedure from informal interviews to the use of standardised questionnaires. Independently of this, a structured summary of the results is just as common as it is indispensable for further steps. The findings on the factual relationships are included in phase 1 "Plan/specify/DPIA" of the DPM cycle (see section D4.1.1).

D4.3 Specifying and Verifying

The basic prerequisite for specifying (see Section D4.4.1) and later verifying (see Section D4.4.3) is the determination of how the protection goals for the data processing under consideration are to be operationalised. Depending on the risk identified (see also Section D3) and with reference to the specific legal requirements, the quality of the processing activities which result from the protection goals must be defined in more detail:

- **Availability** *Within which processes must the availability of which data be ensured for whom? Within which time span must data be available to whom and, if necessary, recoverable?* The influence of the possibility of the proper utilisation of the data in the interest of the data subjects is the benchmark for the concretisation of the protection goal availability.
- **Integrity** *Which data relates to an identified or identifiable person and must therefore be kept intact and up-to-date? How is it ensured that the processes, systems and services are correctly planned, operated and controlled according to the intended purpose?* Again, the interests of the data subjects are the benchmark.
- **Confidentiality** *To whom is the disclosure of which data to be denied? Which processes, systems and services are potentially vulnerable to unauthorised access?* The extent of authorised access is initially to be derived from the respective business processes, regardless of the technology used. This defines the framework within which the measures for the protection of confidentiality against unauthorised

personnel of the controller should be established. The framework for gaining knowledge of data by third parties is determined by the transfer authorisation established in the substantive analysis.

- **Transparency** How and in what form should data processing be kept transparent vis-à-vis data subjects and supervisory authorities? Requirements must be laid down for the information and disclosure obligations pursuant to Art. 12 et seq. GDPR, the notification obligation pursuant to Art. 34 GDPR, the documentation of the processing pursuant to Art. 30 GDPR, the internal documentation of the processing operations and their evaluability as well as the revisability of the processing.
- **Intervenability** *To what extent are data subject rights to be granted?* It is necessary to specify how data subjects can exercise their rights, how to ensure that requests are made in a legitimate manner, what corrective actions can be taken in the processing of personal data (e. g. by rectification, erasure or limitation of the processing of personal data) and in what form data can be transferred by or to other controllers.
- **Unlinkability** *Which purpose changes are permissible? What purposes of auxiliary processes are legitimately derived from core processes?* Statements are only needed for those purposes which the controller actually pursue or intend to pursue. Measures to ensure unlinkability shall be undertaken with the aim to exclude the processing or use of the data for all but the specified legitimate purposes.
- **Data minimisation** *How is the data minimisation requirement implemented?* This includes establishing retention periods for personal data and processes to ensure compliance. Once again, the starting point for the evaluation is the interest of the data subject to limit the burden to the required extent even if within a processing with permissible purposes.
- **Resilience** *Are systems and processes sufficiently prepared for events that cause disruptions to regular processes?* It must be clarified which damaging events, disturbances or attacks can have negative effects for the data subjects and whether countermeasures are available and can be applied in a targeted and timely manner. Due to the cross-sectional character of the objective of resilience, it can be assumed that a sufficient degree of resilience has been achieved with a high degree of maturity in the implementation of the other protection goals.

Once the quality of the protection goals for the processing activity has been specified, technical and organisational measures can be determined. For this purpose, the results of the data protection impact assessment, if one has been carried out, shall be used. The risk to the rights and freedoms of data subjects identified in the risk assessment will determine the course of action to be taken. That result is taken into account for further considerations in three ways.

Firstly, the protection goals can be defined further in a quantitative way. Examples of clarifications are answers to the following questions: For what period and to what degree is the loss of the availability of the data for the persons concerned tolerable? With what delay shall the timeliness of the data be guaranteed? How precise in terms of time must it be possible to retrace the processing subsequently? What is the timeframe in which the controller must be able to safeguard the respective rights of the data subject? How long may data be processed and for what purposes before they are excluded from processing or erased?

Secondly, the result of the risk assessment or the data protection impact assessment forms the basis for weighing the interests of the data subjects against the effort required of the controller. For common processing contexts, the result of such a consideration is outlined by the presentation of typical reference measures in Chapter D1.

Thirdly, the outcome of the data protection impact assessment is included in the assessment of the residual risks that remain after implementation of the measures that can be taken with an effort proportionate to the purpose of the processing. These risks may depend on the interest of third parties or participants who violate the protection goals, whether to gain unauthorised access to data about the data subject, to process it for illegitimate purposes, beyond what is necessary, or in a non-transparent manner.

D4.4 Data protection management process

On the basis of the preparations (see Section D4.2) it can be determined to what extent the protection goals (see Section D4.3) are to be applied and considered.

The DPM process (see Figure 1) is based on the proven PDCA cycle. The Data Protection PDCA cycle (DPM cycle) comprises of the following four phases:

- **Plan**: Plan / Specify / DPIA / Document
- **Do**: Implement / Log
- **Check**: Check / Validate / Evaluate
- **Act**: Improve

The SDM supports the controller in carrying out a threshold analysis and a data protection impact assessment and the resulting selection of a set of technical and organisational measures (target values) by comparing individually selected measures with the generic measures (cf. Section D1) and the measures proposed in the catalogue of reference measures (in **phase 1** of the DSM cycle). The selected measures will be implemented in **phase 2** for ongoing operations. The functional target values resulting from the planning phase are compared with the functional actual values resulting from the ongoing operation (**phase 3a**). This is followed by an assessment of compliance with the legal requirements and any residual risks to the rights and freedoms of the data subjects (**phase 3b**). A level of protection that is too low or residual risks that are judged to be too high must then be

reduced to an acceptable level through appropriate improvements, such as additional measures (**phase 4**).

The assessment made at the end of phase 3 may subsequently form the basis for both the recommendation or request by the supervisory authority and the instructions to the controller to either remedy the deficiencies by means of additional technical or organisational measures or to refrain from the processing activity if legal conformity cannot be achieved or sufficient risk mitigation cannot be achieved by proportionate means (phase 4 of the DPM cycle).

The following graphic shows the entire DPM cycle in which the SDM is integrated.

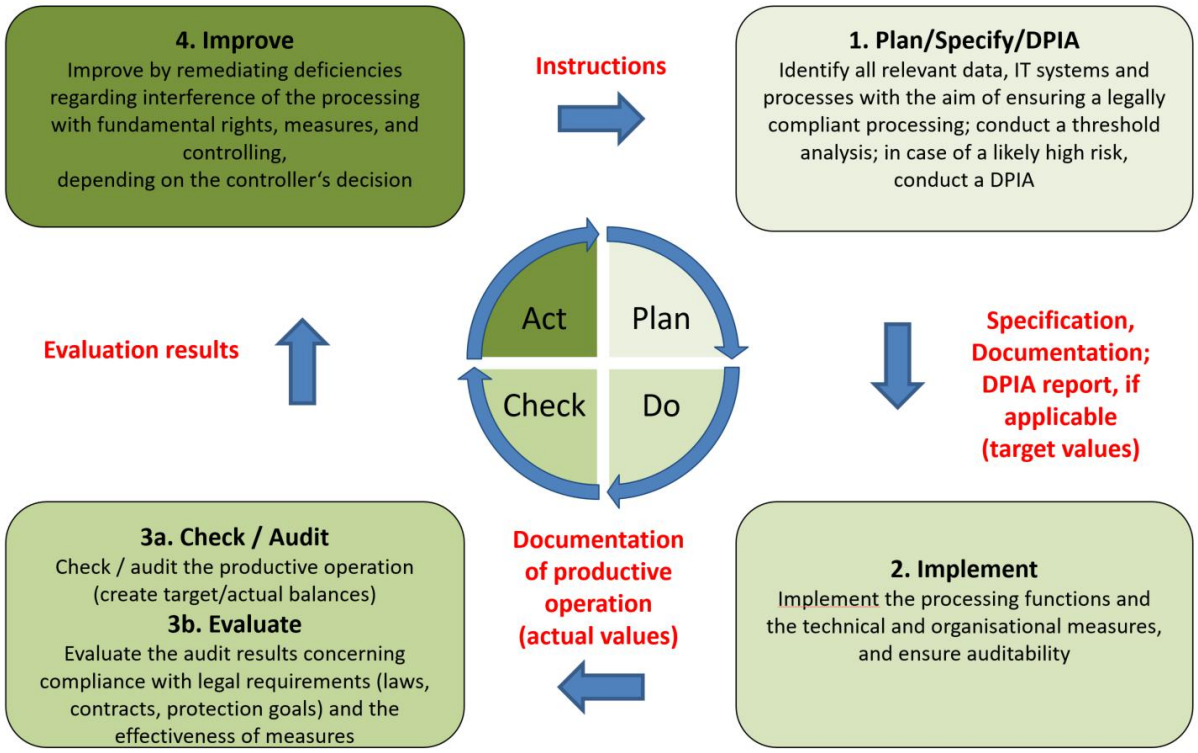

Figure 1: The PDCA data protection management cycle (DPM cycle) as a framework for the application of the standard data protection model in planning, consulting and audit processes

For each processing activity, it will usually be necessary to run through the DPM cycle several times. This applies in particular to the controller when planning processing activities. For example, when commissioning a special process, a first cycle could deal its test operation, a second cycle with its pilot operation and a third cycle with its active operation. The frequency of the runs depends on the extent to which the processing context had to be adapted to the requirements of data protection in the planning phase or as part of an inspection process by the supervisory authority.

D4.4.1 Plan: Specify / DPIA / Documenting

Phase 1 of the planning of a processing activity with person-related data will identify appropriate measures to mitigate the risks of infringing fundamental rights, ensure the

protection of personal data and demonstrate compliance with the Regulation. Functional requirements (target values) must be defined and documented in order to prove the effectiveness of the measures. These are derived from the legal requirements (target) (see Part B Requirements of the GDPR). Only then is it determined which activities of the programs and systems and which events of processes have to be logged.

An essential component of phase 1 is the implementation of a threshold value analysis and, if necessary, a resulting data protection impact assessment (DPIA).

A DPIA shall be carried out if the form of processing, in particular the use of new technologies, is likely to entail a high risk due to the nature, scale, circumstances and purposes of the processing. Whether or not there is likely to be a high risk from a processing activity involving persons must be established beforehand by means of a mandatory threshold analysis (see Part D3.2.1). One result of DPIA is the DPIA report, which identifies the risks and determines the functions and technical and organisational measures to reduce risks. This report often contains additional recommendations on how to proceed when implementing the measures to be taken because Art. 35 GDPR requires the implementation of such remedies.

The controller must decide on the DPIA during phase 1. At the end of Phase 1, they decide on the planned implementation of the functions and the technical and organisational measures.

The execution of a DPIA is not a one-time process. If there are significant changes in the process or processing circumstances that change the assessment of already identified risks or new risks become known, the DPIA has to be reviewed and adjusted. To guarantee this, a continuous, iterative process of validating and adjusting functions is recommended. This iterative process of the DPIA is integrated into the DPM process.

The implementation of the recommended functions and the technical and organisational measures takes place in phase 2 of the DSM.[16]

D4.4.2 Do: Implement / log

In phase 2, the measures recommended from the results of phase 1 are implemented according to the instructions of the controller. Based on the documentation of the functional setpoints, the activities of IT systems and administrators and other relevant events are comprehensibly documented and logged. If a DPIA report is available, the controller must take its results into account when implementing processing activities.

[16] Further details on the systematic conduct of a data protection impact assessment can be found in Short Paper No. 5 of the Data Protection Conference, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, As of: 26. April 2018, last access: 01. April 2019.

When implementing systems and programs, care must be taken to ensure that system documents and protocols can be used to check the functions of the specialist applications and the protective precautions of IT systems and services at the various levels (e. g. client, server). The availability of these documents and logs (actual values) is the prerequisite for the implementation of phase 3 of the DPM.

D4.4.3 Check: Check / validate / evaluate

The core application of the SDM in the DPM cycle is to relate the functional target values determined in the planning phase to the actual values (phase 3a). In addition, the relevant reference measures are compared with the technical and organizational measures that are actually implemented. Deviations from the target must be assessed according to the extent to which they jeopardise the implementation of the principles set out in Article 5 GDPR or the achievement of the protection goals. In an auditing process by a supervisory authority, the analysis carried out up to this point allows to draw conclusions from a failure to achieve the protection goals to (possibly enforceable) data protection deficiencies.

In the practice of testing and assessment, it is often easy to determine whether requirements are not being met because the assigned measures are missing, measures are incorrectly or inadequately implemented, or reference measures have not been correctly applied. The circumstances are more complicated, when the auditee has chosen measures other than those in the catalogue of reference measures. Even if these can be assessed as fundamentally suitable, it must be examined separately whether their concrete form actually corresponds to the identified risk. At this point, the SDM helps to focus the discussion on demonstrating that (or to what extent) the technical or organisational measure taken is functionally equivalent or equivalent in effect to the reference measure.

The starting point for the data protection assessment of a processing activity is the determination of the functional target/actual differences. In the evaluation phase (phase 3b), these differences are translated back into legal terms and compared with the data protection requirements (target). Within the framework of an assessment under data protection law, the deviations identified may become ‘deviations from the norm’. The more serious a deficiency is, the more effectively it must be remedied by appropriate change instructions in phase 4 of the DPM process for a renewed run through of all phases of the DPM cycle. The result of phase 3b consists of assessments that are suitable for bringing about legal and functional improvements.

D4.4.4. Act: Improve and Decide

The deficiencies identified in phase 3b must be formulated in such a way that concrete functional measures can then be taken. These evaluations as results from phase 3 are to be viewed, advised and prioritised by the controller in phase 4. In this phase 4, identified deficiencies must lead to decisions by the controller and the resulting instructions must lead to changes in measures or to new measures, which must then be planned, implemented and

checked in a new cycle. If measures have been taken to remedy all deficiencies, it can be assumed that all deficiencies have been remedied and that the processing activity is legally compliant.

Part E: Organisational Framework

E1 Interaction of SDM and BSI Grundschutz

The SDM is closely related to Grundschutz of the Federal Office for Information Security (BSI). The Grundschutz developed by the BSI makes it possible to identify and implement necessary security measures through a systematic procedure. The BSI standards provide proven procedures for this, the IT-Grundschutz-Compendium concrete requirements. When selecting measures, Grundschutz is primarily oriented towards the protection objectives of Availability , Integrity and Confidentiality known from IT security.

In order to facilitate the application of the SDM, the SDM methodology uses comparable modelling mechanisms to the basic protection methodology. BSI-Grundschutz and SDM are based on the same modelling of a processing activity. The SDM also models the processing activity (business process) with its components systems and services as well as sub-processes and comprehensively considers the element of personal data. The technical and organisational measures to be taken depend on the risk posed by the processing activity and its intensity of intervention. The need for protection is determined from this risk and is also divided into three levels. A direct relationship is established between risk (level) and protection requirements (level) (see section D3). The recommended measures are compiled in the catalogue of reference measures.

The implementation of these security measures is essential for data protection. But the goals of BSI-Grundschutz and SDM differ considerably. When selecting suitable technical and organisational measures, the SDM takes the perspective of the data subject and his or her exercise of fundamental rights and therefore differs from the perspective of basic IT protection. IT-Grundschutz primarily focuses on information security and is intended to protect the data processing institution. The selection of measures under the SDM, on the other hand, is based on the impairment that a data subject must accept as a result of the institution's data processing. Against this background, a distinction must be made between the selection of measures to ensure information security for institutions by responsible bodies and measures to guarantee the rights of data subjects.

In addition to the above-mentioned protection goals known from IT security, the SDM primarily considers the protection goals with data protection relevance from which technical and organizational measures are derived, as in the area of IT security. In this sense, the protection goals of data protection require a somewhat broader understanding in comparison to the protection objectives of IT security, because data protection additionally takes on a broader protection perspective by also considering the risks that the activities of

the organization itself within and outside its business processes pose to the rights and freedoms of natural persons.

As part of the modernisation of the Grundschutz by the BSI, the relationship between data protection and information security was readjusted. The new BSI standard 200-2 refers to the SDM when it comes to determining the risk of an encroachment on fundamental rights and, consequently, the need for protection. The new Grundschutz-Compendium, which replaces the Grundschutz catalogue, contains the new module ‘CON.2 Datenschutz’“ in the section ‘CON: Konzeption und Vorgehensweisen(CON: Concept and Measures’, which describes the demarcation between information security and data protection. The requirement 'CON.2.A1 Umsetzung Standard-Datenschutzmodell (Implementation of the standard data protection model)' states that consideration should be given to whether the standard data protection model is applied and that reasons should be given for any failure to consider all protection goals and for any failure to apply the SDM methodology and reference measures.

BSI-Grundschutz and SDM thus complement each other ideally and jointly provide the information required to demonstrate compliance with the principles governing the processing of personal data (accountability pursuant to Art. 5 para. 2 GDPR).

E2 The operating concept for the Standard Data Protection Model

E2.1 Introduction

The operating concept is designed to give the users of this model competence and confidence in handling it. This means that it is necessary to clarify who is responsible for the SDM, which version is currently valid, and which version was used, and where this current version is available. The operating concept regulates three aspects:

- Clarifying roles and responsibilities with respect to the model,
- Ensuring the applicability of the SDM,
- Creating transparency regarding the publication and development of the model.

E2.2 Contractor, Project Management, User

The contracting authority for the development and maintenance of the SDM are the members of the *Conference of the Independent Data Protection Authorities of the Federation and the Länder (Data Protection Conference - DSK)*. DSK is the owner and publisher of the SDM, which includes both the methodology and the catalogue of reference measures.

The SDM is developed and maintained by the DSK (AK Technik) working group " *Technische und organisatorische Datenschutzfragen* (Technical and organizational data protection issues)". The AK Technik is responsible for the project management.

The SDM can be used both by the sixteen State Data Protection Officers, the Bavarian State Office for Data Protection Supervision and the Federal Data Protection Officer within the framework of their statutory advisory, verification and sanction activities (user group 1) and by the controller and processors for the planning and operation of the processing of personal data as well as the data protection officers within the framework of their advisory and verification activities (user group 2).

The model will be further developed both as part of the practice evaluation and according to functional requirements as follows:

- Creation and maintenance of the SDM, which also includes the catalogue of reference measures;
- Provision of the SDM and the catalogue of reference measures;
- Processing of change requests (CRs) to the SDM, which can be introduced by both user groups and for which the DSK must decide on their acceptance;
- Ensuring the quality of the work results;
- Version control for the SDM;
- Project management, including
  - Provision of a Single Point of Contact (Service desk)
  - Operation of CR tracking
  - Moderating discussions
  - Administration of necessary means (website, project platform)
- Public Relations

E3 Changes in the different SDM versions

E3.1 Changes from V1.1 to V2.0 (As of 17. April 2020)

The version SDM 2.0 now comprises of five parts:
Part A: Description of the SDM,
Part B: Compilation of the requirements of the GDPR,
Part C: Systematisation of the requirements of the GDPR through protection goals,
Part D: Practical implementation,
Part E: Organisational framework conditions, operational concept, history, reference to reference measures catalogue.

Part A describes the purpose, scope and structure of the model, which content has not changed since the previous version. The SDM comprises of seven protection goals, a strategy for assessing risks and protection requirements, and the three functional components of a processing activity. New is the supplementation of the ‘services’ mentioned in the GDPR with the ‘IT systems’.

Part B adjusts the SDM V2.0 more to the GDPR requirements compared to the previous version. In particular, all individual concrete measures mentioned in the GDPR to implement the rights of data subjects have been taken into account. In addition, a chapter on ‘Consent management’ and ‘Implementation of supervisory orders’ has been added.

In Part C, the protection goals are assigned – as before – to the principles of Art. 5 GDPR as well as to the many individual legal requirements from Part B. The protection goals are also assigned to the principles of Art. 5 GDPR. The SDM 2.0 thus guarantees the complete consideration of operational requirements of the GDPR much better than before. This chapter replaces the assignment of protection goals and articles of the GDPR from SDM-V1.1/S. 21, Tables 1 and 2.

Part D represents the practical implementation; here the most comprehensive changes have been made compared to the previous version. In the chapter on ‘Risk and Protection requirements’, the conceptual innovation to V1.1 is a clear presentation of the relationship between the need for protection and risks: The protection requirements of a person arises from the risks that a processing activity involving a person would generate without technical and organisational measures. While protection requirements thus determined for the data subjects remains constant, the risks can be reduced – through the design of the processing activity and the operation of technical and organisational measures; this reduction must take place to a responsible level of protection or residual risk.

The chapter on ‘Data protection management’ has been added. A data protection management (DPM) represents a methodical link between the operational and legal requirements of an organisation and the technical functions and technical and organisational measures. Therefore, the presentation of a DPM should always be part of the methodology. This chapter also refers to the performance of a data protection impact assessment pursuant to Art. 35 GDPR and clarifies the mutual relationship between data protection impact assessment and data protection management. As an essential component, it contains a brief description of a Deming cycle that has been specifically adapted to the data protection audit requirements. The conceptual innovation consists in the fact that the exact location of the reciprocal reference of target/actual test procedures, which concern technical and organisational target values, and evaluations of normative target/actual assessments, is shown. Each of the four phases generates products (specifications, documentations, assessments, instructions of the responsible person) as output, which forms the input of the following phase. This chapter takes many aspects from chapter SDM-V1.1/p. 34, ‘Testing and Advising’ and replaces them.

Particular attention was paid to a more consistent use of the term ‘processing activity’ (formerly ‘procedure’), which is a key term in the GDPR. While the term ‘processing’ is defined in Art. 4 para. 2 GDPR, the term ‘processing activities’ is used in Art. 30 para. 1. In SDM V2.0, the generic term ‘processing activity’ is now used, with ‘processing’ (such as

collection, saving, querying) as components. The term ‘processing operation’ may also be used to designate such sub-processes of a processing activity.

With Version 2.0b the chapterE6 was supplemented with instructions for use concerning the obligation of usage of the Catalogue of reference measures. This was adopted by the 99. Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder on the 17. April 2020

E3.2 Changes from V1.0 to V1.1 (as of 26. April 2018)

The following changes concern the whole text:

- In the present version, the SDM refers exclusively to the GDPR; the references to the BDSG and the state data protection laws have been removed. References to the revised Federal Data Protection Act (“BDSGneu”) and the amended state data protection laws may have to be newly established. The right to create these references is reserved for a further update of the SDM.
- The term ‘procedure’ has in many places been replaced by the term ‘processing’ or ‘processing activity’ as used in the GDPR, and the term ‘fundamental right’ has also been changed to the GDPR formula ‘rights and freedoms of persons’.
- Care was taken to ensure that the SDM as a whole was also internationally connectable, whereby references to rulings of the Federal Constitutional Court (“BVerfG rulings”) were retained.
- An addition to this chapter which lists the changes to the previous version.

Significant changes in the individual chapters

‘Chapter 1 Introduction’ has been completely revised; the exclusive reference to the GDPR is new.

Chapter 2 ‘The purpose of the standard data protection model’ was completely revised; it became clearer that before the SDM could be used to select and configure technical and organisational measures, the legal balancing and necessity processes and an initial risk analysis had to be carried out.

Chap. 5.5 ‘Further derived protection goals’ was deleted without replacement.

Chapter 6.2 ‘Embedding the protection goals in the BDSG’ and ‘Chapter 6.3 Embedding the protection goals in the national data protection laws’ and all subchapters were deleted. The following passage was added in ‘Chapter 6.2 Embedding the protection goals in the GDPR’: "In an update of the manual it is planned to supplement the embedding of the protection goals in the EU Directive on Data Protection in the Police and Justice Sector and the ePrivacy Regulation of the EU which is currently being coordinated".

Chapter 8 ‘The process components’ was completely revised. On the one hand, it was necessary to switch to the concept of ‘processing’ or ‘processing activity’ and, on the other hand, practical experience has shown that there is a need to clarify the different levels of understanding of the concept of ‘processing’ and which aspects should be taken into account when defining a purpose or purpose limitation.

Chapter 9 ‘The need for protection’ has been completely revised. The GDPR already contains a certain amount of methodological guidance on risk identification, which is why guidance on the methodological identification of risks or the need for protection has become redundant.

E4 Keyword Index

E5 List of abbreviations

Sect.	Section
AK Technik	Working group "Technical and organisational data protection question" of the DSK
Art.	Articles
Art.29 working group	Artikel-29-working group
BSI	Bundesamt für Sicherheit der Informationstechnik
CON	(Name of a module in the BSI compendium)
CPU	Central Processing Unit
CR	Change Request (Änderungsantrag)
DPIA	Data Protection Impact Assessment (DPIA)
GDPR	General Data Protection Regulation Data Protection Conference
DSK	Data Protection Conference
DPM	Data Protection Management
ECJ	European Court of Justice
ICT	Information and communication technology
IT	Information Technic
Chapt.	Chapter
LAN	Local Area Network
lit.	Letter
NAS	Network Attached Storage
NEGS	National E-Government Strategy
No.	Number
PDCA	Plan Do Check Act Cycle
SAN	Storage Area Network
SDM	Standard-Datenschutzmodell

SPoC	Single Point of Contact
c.f.	Compare
WP	Working Paper (of Art.-29-Group)
e. g.	For example

E6 Appendix Catalogue of reference measures

The catalogue of reference measures in the Annex forms part of the SDM. It contains a description of technical and organizational measures that will contribute to fulfilling the legal requirements described in part B. The measures were selected assuming typical processing situations and were combined into modules. Implementing the specified measures constitutes good data protection practice. In many cases, it is appropriate and proportional.

The enumeration of measures in the modules is not exhaustive. By including a measure in a module, the Conference does not issue a binding statement regarding the obligation to implement it. Nevertheless, such an obligation will often exist, taking in to account the factors that need to be considered by legal requirement. Among these factors, depending on the applicable legal norm, are 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. However, the differentiation made in the text regarding the binding character of specific measures – expressed by the modal verbs MUST, SHALL, and SHOULD – merely constitutes an assessment of how critical the implementation of the measure in question is, to ensure that the requirements posed by the GDPR are met in a typical processing situation.

Controllers and processors are obligated to analyze the peculiarities of their processing operations, to conduct a risk assessment, and, on this basis, to select and implement appropriate technical and organisational measures both at the time of the determination of the means for processing and at the time of the processing itself. In doing this, they are free to desist from the implementation of measures that are not appropriate or proportional under the concrete circumstances, and to replace any measures listed in the modules by other measures having the same or a similar effect. On the other hand, an obligation might arise to complement the measures listed in the modules by additional ones.

As the Annex constitutes a reference catalogue, however, users of the SDM will have to document if, in how far, and why they have decided to implement measures of the modules in a way different from the recommendations of the SDM. In these cases they will have to ensure an appropriate level of protection for the data subjects.

The Standard Data Protection Model

A method for Data Protection advising and controlling
on the basis of uniform protection goals

Version 2.0b (english version)