The Standard Data Protection Model

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

Version 3.0a
(english version, V1.0c)

IMPRINT

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

Version 3.0a
Adopted by the 104. Conference of the Independent Data Protection Supervisory Authorities ofthe Federation and the Länder on the 24. November 2022

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,
- Intervenability.

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

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.

information security who are familiar with the Grundschutz concept2, 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.

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

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.

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

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.

GDPR, the controller must create the conditions for granting these rights through 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).

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

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

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 context 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 pursuant to 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. 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

---

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.

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 context 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
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 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
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 a concept for role-based access control 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 No. 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 and the information requirements pursuant to Art. 12 para. 1 GDPR.

The function of the complete documentation of a processing is to make all relevant components of a processing activity auditable due to the existing accountability, in order to be able to subject these to a data protection evaluation. Auditability 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 comparison.

This target/actual comparison 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 compliance as a whole under the aspect of whether the correct measures are selected appropriately and operated with the necessary effectiveness.

D2.1 The subdivision of a processing activity into operations or into the phases of the life cycle of the data

To examine a processing activity from a data protection perspective, it is recommended to break it down into the relevant sub-processes or processing operations. The definition of ‘processing’ in Art. 4 No. 2 GDPR does – especially but not exhaustively – list 14 elementary operations which, when sequenced in line, represent a possible life cycle of a processing of personal data: A processing activity starts with the context in which the data are collected, followed by their use and ends with the deletion or destruction of the data.

In principle, each of the elementary processing operations can be assessed with regard to its compliance with the GDPR requirements. However, in audit and advisory practice, e.g. in the context of a DPIA, it is usually sufficient to conflate some of the processing operations mentioned in the GDPR due to their similarity. Furthermore, there are processing operations that can be added to the catalogue of Art. 4 No. 2 GDPR and distinguished from the other

elementary operations. In order to examine a processing activity from a data protection perspective, it is generally recommended to examine it in relation to the following nine groups of operations, which are to be understood as sub-processes of that processing activity:

1. Collecting (Co) (collecting, recording, also receiving and generating)
2. Preparing (Pr) (organising, arranging)
3. Storing (St) (saving, also filing of paper documents)
4. Editing (Ed) (adapt, change)
5. Using (Us) (read out, query, use, also filter and evaluate)
6. Making available (Ma) (disclosure by transmission, dissemination or other form of making available)
7. Merging (Me) (matching, linking)
8. Restricting (Re) (also blocking)
9. Removing (Rm) (delete, destroy)

This list of operations is not exhaustive. The GDPR also mentions archiving, profiling, scoring, anonymization or pseudonymisation as specific processing operations. These processing operations are usually composed of operations from these nine groups. If further groups or sub-processes are identified when a processing activity is broken down into the groups of operations listed above, these must also be considered.

The total of all elementary operations can be considered as a 'series of operations' in the life cycle of personal data during its processing, in which four phases can be distinguished chronologically, although in some cases only a certain subset of the elementary operations can be sufficient. The collection phase (operation group 1) is followed by the storage phase (operation groups 2 to 3), and then by the usage phase (operation groups 4 to 8). The performance of the phases of storage and usage of personal data can happen several times and cyclically. Finally, the phase of removal (operation group 9) marks the end of the life cycle of the processing of specific personal data (see Figure 1).

Elemental Processing activities purs. Art. 4 para. 2 GDPR	Groups of processing activities	Phases of a data life cylce	Comment
1. Collection 2. Recording	1. *Collection*	1. Collection	Raw data of natural persons (data subjects) are in the hand of a recipient (controller).
3. Organisation 4. Structuring	2. *Preparing*	2. Data storage	The data are stored in a structured manner and are available in a status in which they can be processed.
5. Storage	3. *Storing*		
6. Adaption or Alteration	4. *Editing*	3. Data use	The data are accessible for processing in compliance with the law, if necessary also for authorised third parties. They can be linked to other processing activities and the access to them can be restricted.
7. Retrieval 8. Consultation 9. Use	5. *Using*		
10. Disclosure by transmission 11. Dissimination or otherwise making available	6. *Making available*		
12. Alignment or combination	7. *Merging*		
13. Restriction	8. *Restricting*		
14. Erasure or destruction	9. *Removing*	4. Data destruction	Data will be irreversibly removed or physically destroyed.

Figure 1: Processing operations and phases of a data life cycle according to Art. 4 No. 2 GDPR

This modelling of a processing activity into its individual operation groups and phases of the life cycle of the personal data makes it possible to specifically identify and examine the data protection requirements and risks. Considering the nature, scope, context and purposes of the processing as well as the risk to the rights and freedoms of natural persons, a decision must be made as to whether an operation- and/or phase-specific investigation of a processing activity should be carried out.

Figure 2 contrasts the terms used in Art. 4 No. 2 and Art. 30 of the GDPR with the taxonomies frequently used in the public and non-public sectors. It should be noted that the processing of personal data may not be part of every administrative procedure or business process. Furthermore, there may be operations or activities within specialised procedures or business processes in which no personal data is processed.

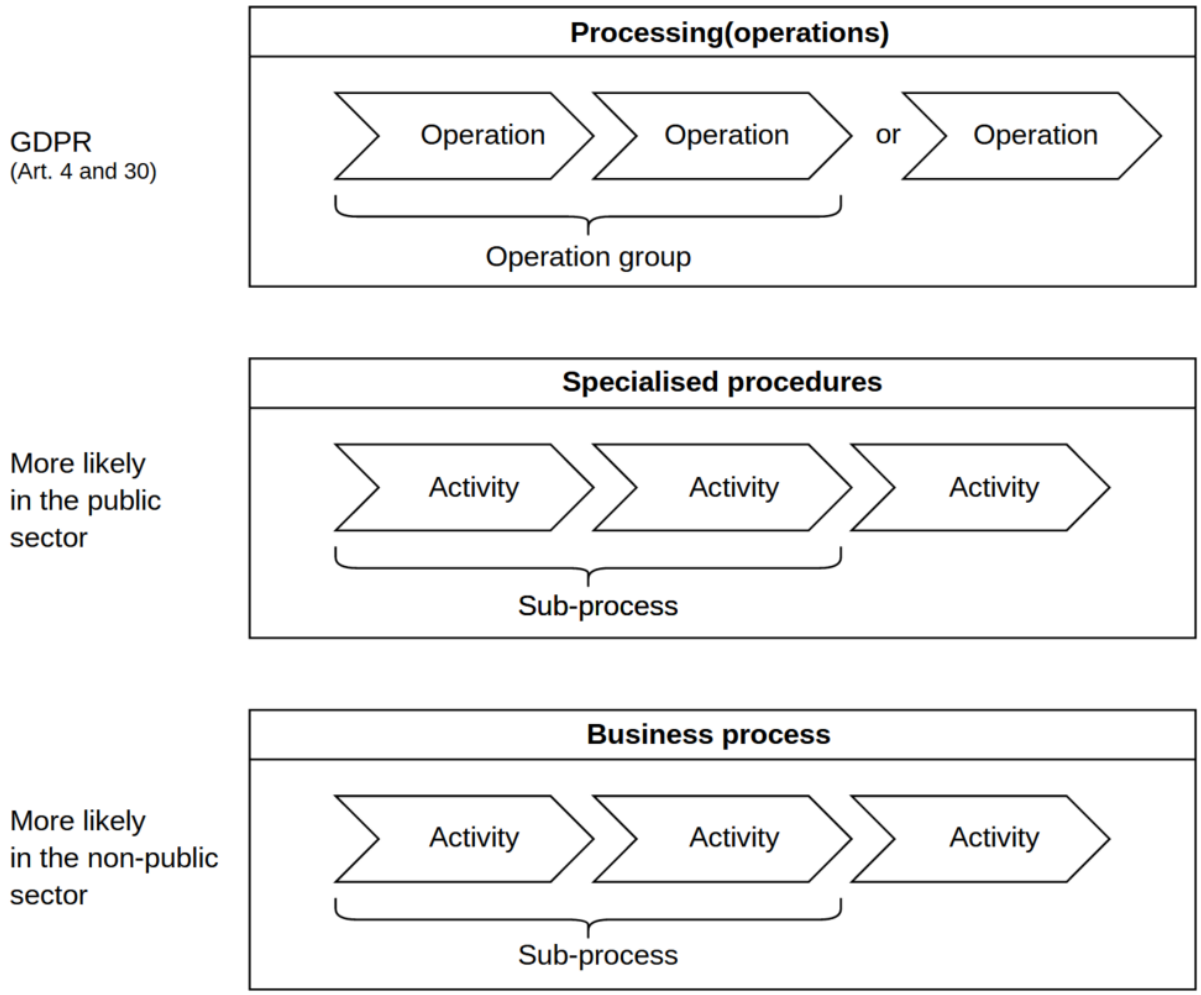

Figure 2: Taxonomies regarding 'processing operations' (GDPR)

D2.2 Levels of a Processing Activity

When designing or reviewing a processing activity of personal data, it is useful to distinguish between at least three different levels of representation of significant aspects or components to fully understand the processing activity. It is essential to understand that a 'processing activity' is not, for example, the same as the use of a particular technology or specialised software application.

Level 1 is the processing of personal data in the sense of data protection law. This processing takes place, for example, within the context 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 specific functional sequence of the processing activity. This is the logical level of a processing activity where personal data necessary for a processing activity and the legal requirements are identified. The controller defines appropriate roles, responsibilities and roll-based access controls 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 design 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 case handling or task as well as the IT application(s), which can also be described more precisely as the 'specialised application of a specialist procedure'. The case handling/task and the specialised application must fully comply with the relevant legal and functional requirements (of data protection). The **specialised application must ensure purpose limitation**. The processing in the specialised application must exclude any additional data or additional forms of processing from level 1, even if they may be particularly convenient from a functional point of view. The aim is to minimise the risk of undermining the purpose limitation or overstretching the purpose.

Level 3 is the IT infrastructure that provides the functionality that is used by a specialised application at level 2. 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, as well as the communication infrastructure of an organisation such as the telephone, LAN or Internet access. Again, these systems must each be designed and used within a processing activity in such a way that **purpose limitation** continues to be effective. For purpose limitation or the separation of purposes to be enforced at this level, technical and organisational measures are typically necessary.

D2.3 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 proven useful to consider two further aspects in order to achieve a sufficient purpose limitation of the processing activity:

- In addition to the purpose, the aspects of **purpose differentiation** and **separation of purposes** shall 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 processing activities from each other and, in particular, the separation of data, systems and services as well as processes at the IT level.
- The aspect of **purpose limitation** must also be considered. On the one hand, the purpose limitation of a processing operation must be ensured by means of its appropriate functionality and by means of an appropriate selection of the production or user data to be processed (horizontal design). However, the purpose limitation of a processing must also be ensured by an appropriate cross-level design (see section D2.1) (vertical design). For example, it is usually not covered by the purpose and not operationally necessary that, in addition to authorised administrators and their superiors, IT administrators who manage access rights, for example at the level of a database, are also allowed to see the content of the processed data.

D2.4 Components of processing or processing activity

The requirements of the GDPR directly result in the components data, systems, and services. However, in the concrete modelling of processing activities involving individuals, it is necessary to consider the following three components:

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 modelled as a business process or specialised procedure and consists of individual processing steps. Individual processing operations are, for example, collection, recording, classification or storage until erasure or destruction (cf. Art. 4 No. 2 GDPR). These processing steps are modelled or implemented as sub-processes.

In methodological terms, the priority is the personal data whose necessity to be processed must be assessed in advance in relation to the intended purpose.

The concrete functional design takes place at level 1, where the risk to the rights and freedoms of natural persons ("risk of processing") or the need to protect data subjects must be determined by the controller, as well as the risk level of the processing. This risk level is decisive for all data, systems and processes used in a specific 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 protection needs.

For these three core components – data, systems and services as well as processes – the following special properties, among others, play an additional role that must be taken into account:

It is necessary to consider the properties of **data formats** that are used to collect and process data. Data formats can have an influence on the quality of the implementation of the protection goals, e.g. in cases where it cannot be considered conclusively clarified what data is contained in files with certain formats. For example, text files may contain supposedly deleted data that does not appear in the printout; graphic files may contain metadata, e.g., camera model, location and time of recording; or relevant information in graphic, video and audio files may fall victim to compression.

In terms of the systems involved, it is necessary to consider the **interfaces** between a specialised application and the use of level 3 IT systems, and especially to other systems which are not within the intended scope of the application. In addition to these vertically oriented interfaces, horizontally oriented interfaces must also be taken into account, which pose a risk for purpose limitation. The identification of the existence of interfaces as well as the documentation of their properties are of crucial importance for the legal accountability, controllability and auditability of data flows.

For each processing activity and its components, especially for the sometimes difficult to grasp processes across different systems, it is important to clarify the **controllership** and to document it in the records of processing activities pursuant to Art. 30 GDPR. According to Art. 4 para.7 GDPR, a Controller is "(...) a natural or legal person, public authority or agency (...) which alone or jointly with others determines the purposes and means of processing (...)". Tasks resulting from the responsibility may be delegated in the form of individual responsibilities. These responsibilities are typically formulated and assigned as roles in a comprehensive concept of roles and responsibilities. The responsibility of a process owner can extend to individual processing operations (sub-processes) 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 performs its tasks in accordance with the instructions of the controller in a data protection compliant manner.

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

D2.5 Overview of SDM modelling techniques ('SDM cube')

In the previous chapters, various SDM modelling techniques were introduced. In Part C, the requirements of the GDPR (Part B) were systematised by 7 protection goals. Chapter D2.1 introduced nine groups of elementary operations (operation groups) and four phases of a data life cycle, on the basis of which a processing activity can be examined taking into account its sub-processes. Chapter D2.2 recommends examining a processing activity at three levels. Chapter D2.4 introduces three components that can be used to model a processing activity.

The relationship between the levels and the components of a processing activity is shown schematically in figure 3. The (sub-)processes of a processing activity are located on level 1 (specialised procedures). The systems and services are located on level 2 (specialised application) or level 3 (infrastructure), depending on their technical characteristics. Data components can be found on all three levels. On level 1, it is mostly the data categories that are processed within the context of the processes. On levels 2 and 3, further (technical) data can be processed and identified if necessary. In addition, data formats and data structures are specified and implemented at these levels.

The operation groups or phases of a data life cycle can be used to break down a processing activity at level 1 into its sub-processes, which may be linked in a complex manner in individual cases.

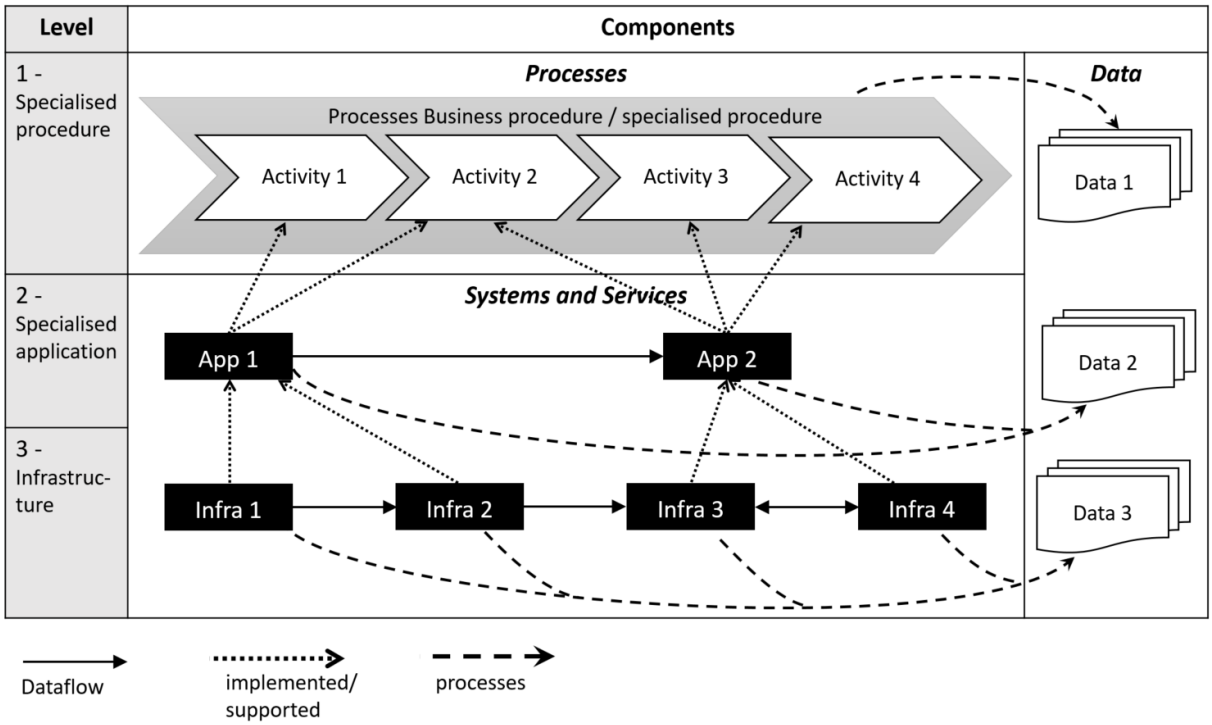

Figure 3: Relationship between levels and components of a processing operation

The subject of a data protection impact assessment pursuant to Art. 35 GDPR (and, where applicable, a data protection certification pursuant to Art. 42 GDPR) is a *processing operation* or are several similar processing operations. A processing operation is a sub-process or one or more processing activities (business process) including the implementation of the process on levels 2 and 3 by the systems and services used and the personal data processed. An adequate examination and assessment of a processing operation is only possible by including all components at the different levels.

The operation groups or the phases of a data life cycle can be used to fully identify and model individual processing activities at the three levels. A sub-process on level 1 may include several processing operations of different operation groups. These processes were realised on levels 2 and 3. Furthermore, additional (technical) processing can take place on levels 2 and 3. In figure 4, this connection is established by annotating the components of the schematic representation from figure 3. Each component is annotated with the respective operation group(s) that correspond to the actual type of processing of personal data It should be noted that on levels 2 and 3, the personal data of the levels above are also processed.

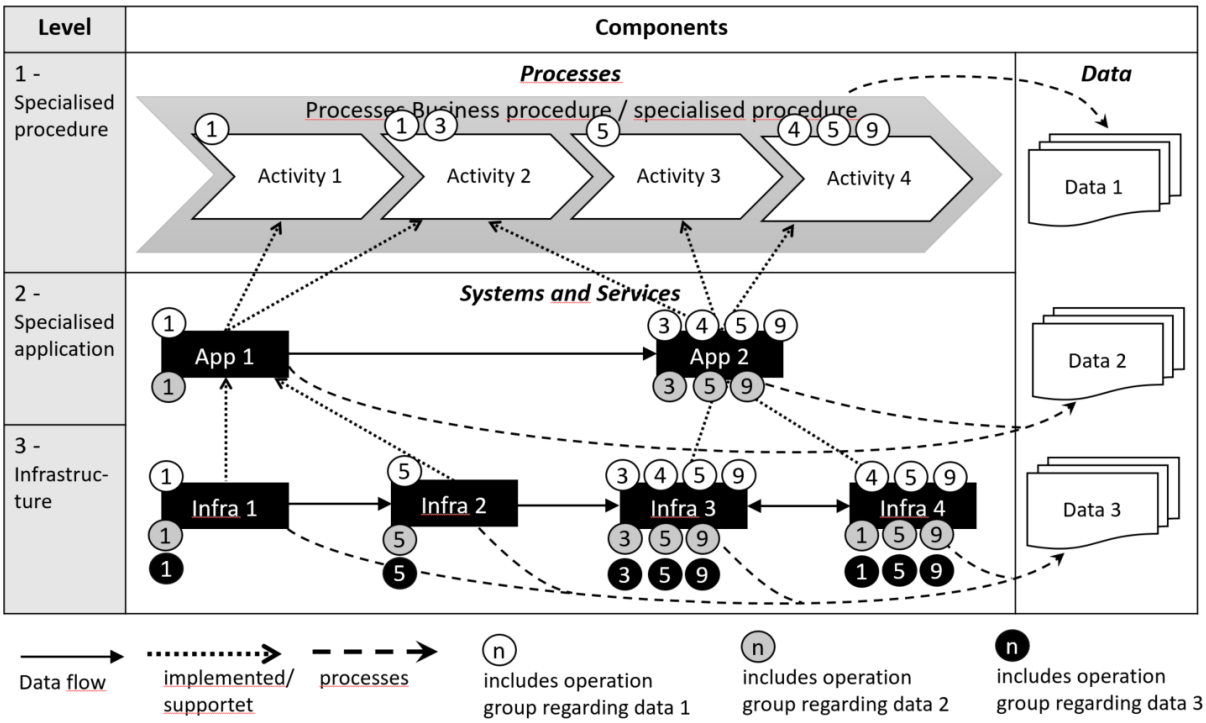

Figure 4: Annotation of the operation groups to the components

The audit of a processing activity regarding the implementation of data protection requirements can be carried out based on the protection goals from Part C, or based on the requirements of the GDPR from Part B. To cover all components and levels in such an audit, the protection goals can be added as an additional axis/dimension to the modelling of a processing activity. The resulting SDM cube (cf. **Fehler! Verweisquelle konnte nicht g efunden werden.**) provides support for a systematic and complete examination of a processing activity.

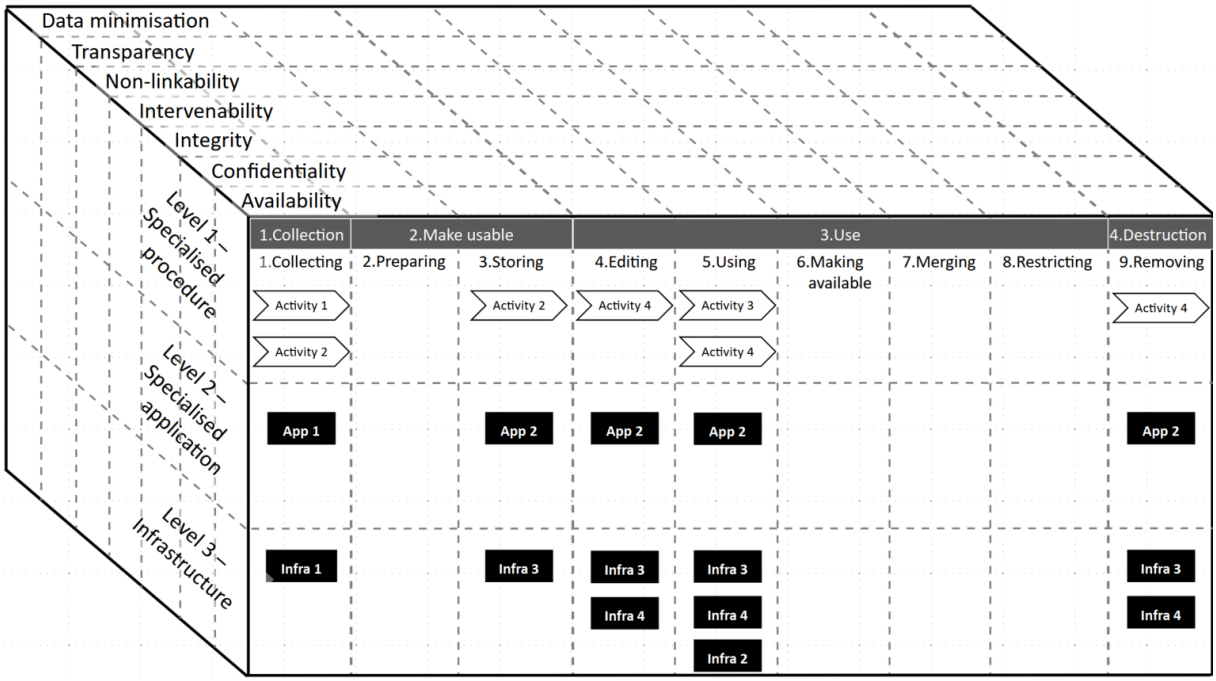

Figure 5: 'SDM cube', schematic representation.

On the x-axis, the operation groups or life cycle phases are plotted. On the y-axis, all components of a processing activity are plotted, sorted by the three different levels of of a processing (level 1 'specialised procedure'/"business process", level 2 'specialised application' and level 3 'technical infrastructure', see chapter D2.2). The components, processes as well as systems and services, belonging to a group of operations or phase are found on the respective level. The assignment of a process or a system or service to an operation group or a phase is done depending on the processed data (cf. annotations in figure 4). Figure 5 shows this assignment as an example based on figure 4 for 'Data 1'. It should be noted that not every processing activity includes all groups or phases. Furthermore, the components may be assigned to several operations or phases (e.g., if a system or service is involved in the implementation of several processes). These components must then be examined regarding all assigned operations or phases. The z-axis lists the seven protection goals which contain the requirements and serve to generate the risks in relation to the risk level.

For the analysis of a processing, it makes sense to always use and examine two dimensions of the cube first:

a) If one looks at the operation groups or phases together with the protection goals, it becomes apparent that there are specific requirements for operations and phases that must be dealt with. For example, the protection goals for collecting data regularly have different requirements than those for transmitting or erasing data.

b) Looking at the three levels of processing together with the protection goals, it becomes clear that at the highest level of processing in terms of data protection law ('specialised procedure' / 'business process') there are regularly requirements in other forms or levels of

abstraction than at the level of specialised applications or at the level of infrastructure. At each level, the level-specific form for transparency must be defined. At level 1, for example, there is the requirement of technical verifiability for the data subjects (e.g. 'acknowledge result'). At level 2, this requirement for verifiability presupposes a special code, stored as a 'specialised protocol'. On level 3, e.g. in a database, a technical protocol is required.

c) Looking at the operation groups and the levels of a processing together helps to understand how requirements and risks on the specialized procedure level can interact with requirements or risks on the specialised applications levels as well as the infrastructure level in a selective and structurally reinforcing way. Based on the processing operation, resources planned or used can be functionally assigned to each processing step. This helps to take a comprehensive look at the various IT components. In this way paths become visible along which inheritable or emergent risks are 'propagated' , blocked or shared.

The SDM cube thus presents an overall picture for analysing the risks of a processing activity.

This overview is particularly useful for complex processing activities. It systematically ensures the completeness of the analysis, the need for action and the evidence of the implementation of data protection requirements and the handling of risks. In addition, the cube can provide valuable support for data protection impact assessments and certifications of processing operations.

For less complex processing operations with a low or normal risk level, it may be sufficient to refer only to the four lifecycle phases of a processing activity and to analyse the respective operations within the phases in a coarsening manner as a heuristic. Furthermore, not every processing activity will always include all nine groups of operations. In general, all audit obligations that are derived from the GDPR and addressed with the help of the cube should also be analysed and assessed. However, this does not necessarily mean that specific measures are required for each individual area.

D3 Risks and Need for Protection

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

The Data Protection Conference's Short Paper No. 18 "Risiken für die Rechte und Freiheiten natürlicher Personen" [9] explains the concept of risk in the context of the GDPR and shows in general terms how risks to the rights and freedoms of natural persons can be determined and assessed in terms of their legal consequences.

A risk within the meaning of the GDPR is the possibility of the occurrence of an event which may cause damage to the rights and freedoms of natural persons (including unjustified

9 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, as of: 26.04.2018, last accessed: 29/07/2019.

interference with rights and freedoms) or result in damage for one or more natural persons. It has two dimensions: First, the severity of the harm to the rights and freedoms of data subjects and second, the likelihood that the event and the harm will occur.

According to recital 75, the possible damage to the rights and freedoms of natural persons includes physical, material and non-material damage. In the following, we will generally speak of damaging events. A damaging event can damage or impair various rights and freedoms and possibly lead to further damaging events. Unlawful processing activities, especially those that 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 an event of damage. They may result in 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 in relation to the nature, scope, context and purposes of the processing.

It is the task of the controller to identify, analyse and classify these risks and to take measures to mitigate them (see Chapter D4 Data Protection Management with the SDM).

This chapter D3 provides guidance on how to determine the data protection risk of a processing activity. It also establishes the connection between the risks posed by a processing activity and the need for protection of individuals regarding the processing of personal data (Art. 1 para. 1 GDPR) caused by it 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 hand, with the aim of enabling the determination of appropriate and proportionate measures. Determining the level of risk is the prerequisite for being able to determine technical and organisational measures and the necessary degree of their effectiveness with which risks can be eliminated or at least reduced and processing can be carried out in compliance with data protection. In general, the following rule applies: The higher the risk, the more prudently the processing activity must be designed and the more effectively the corresponding concrete technical and organisational measures must be applied, 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 used, because according to the definition in Art. 4 No. 2 GDPR, processing operations are individual operations or a series of operations. For each processing activity, the principles of processing personal data formulated in Art. 5 GDPR must be observed. The SDM ‘consolidates’ these principles into protection goals , that incorporate further operational

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

requirements of the GDPR. In principle, every processing activity creates risks for data subjects by the mere fact of processing personal data.

In contrast to general risk management and to 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 by means of suitable and adequate 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 from Art. 5 GDPR, and to accept the resulting risks. The instruments of risk acceptance or risk transfer known from the area of information security are not available to the controller in the context of data protection law. There is room for manoeuvre in the selection and manner of implementing requirements with the help of technical and organisational measures, which are required to an appropriate extent (Article 5 No. 1 lit. d 'reasonable steps', lit. f 'appropriate security'). At this point, 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 thus the interests of the data subjects have been adequately taken into account, can the remaining residual risks be accepted by the controller.

In the context of operational data protection, a distinction can be made between four types of risk, which are to be reduced with different types of protective measures:

- Risk type A: The encroachment on the fundamental rights of natural persons caused by the processing operation is not of a sufficiently minor nature.
- Risk type B: The measures to reduce the intensity of the interference of a processing operation are, in relation to the objectives of the safeguards, not complete or are not operated with sufficient effectiveness or are not continuously monitored, checked and evaluated to a sufficient extent.
- Risk Type C: The measures required by information security (cf. e.g. IT-Grundschutz according to BSI) are not complete or are not sufficiently effective or are not constantly controlled, checked and assessed to a sufficient extent (see the differentiation between operational data protection and IT security in chapter E1).
- Risk type D: The information security measure is not sufficiently operated in accordance with data protection, in the sense of risk type A and risk type B.

The examination of the proportionality of the interference with fundamental rights of a processing operation is not covered by the SDM. This legal examination, as well as the examination of the legal basis according to Art. 6 and, if applicable, 9 of the GDPR, must take place before the SDM is applied. Thus, the treatment of the aforementioned risk type A is not directly subject to the application of the SDM.

Article 35 of the GDPR requires the Controller to carry out a Data Protection Impact Assessment for the intended processing in case of a 'likely high risk' to the rights and freedoms of natural persons. 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 to classify 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 is a '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 purpose of the threshold analysis is to determine whether a processing activity is likely to result in a high risk to the rights and freedoms of individuals and thus requires a DPIA . The following procedure is suggested for identifying a likely 'high risk' from a processing activity, although the order does not necessarily have to be followed:

1. Check whether the processing activity for which the risk is to be determined is included in the 'mandatory list' of the data protection supervisory authorities pursuant to Art. 35 para. 4 GDPR. If so, then there is likely to be a high risk. (For the non-public sector: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf, as of: 17.10.2018, last accessed: 01/04/2019.

2. Check 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, there is likely to be a high risk.

3. Check whether the processing activity has any of the characteristics listed in the list of 'likely high risk' processing activities in Working Paper 248 rev. 01 [11] of the European Data Protection Committee. If at least two of the entries apply, it can be assumed in most cases that there is a likely high risk given. However, a high risk may also exist even if only one of the criteria is met.

1. *Evaluation or scoring*
2. *Automated decision-making with legal effect or with similar significant effect*
3. Systematic monitoring
4. *Sensitive data or data of a highly personal nature*
5. *Data processed in a large scale*
6. *Matching or combining datasets*

11 This working paper was originally adopted by the EDSA's predecessor institution, the Article 29 Working Party, and later by the EDSA with confirmation 1/2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, as of: 13.10.2017 (revision 0.1; last accessed: 01/04/2019)

7. *Data concerning vulnerable data subjects*
8. *Innovative use or applying new technological or organisational solutions*
9. *When the processing prevents data subjects from exercising a right or using a service or a contract*
   (from: WP 248 of the Art. 29 Working Party, from page 10 f).

4. Check whether the nature, scope, context, or purposes (Recital 76 GDPR) of the processing activity increase the risk for data subjects. For this purpose, it is advisable to include relevant practical experience and concretising court rulings in the examination of a possibly existing high risk.

D3.2.2 Risk Identification

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

a) What damage may occur to data subjects based on the data being processed?
b) By what, i.e. through which events can the damage occur?
c) By what actions and circumstances can these events occur?

This step may, in exceptional cases, identify risks that could have very serious consequences for the data subjects, such as danger to life and limb. In such cases, it makes sense to assume a very high need for protection of the persons (see section D3.3). However, the technical and organisational measures proposed by the SDM are not designed for this, so that in such a case, as in the case of a high need for protection, the possible measures must always be considered individually to establish an appropriate level of protection. 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 for dealing with these risks (https://www.bsi.de). Essential aspects of basic protection measures concern 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. When coordinating measures for information security and operational data protection, it is very important to ensure that the protective measures that are operated for IT security are themselves set up in a data protection-compliant manner (e.g. video surveillance for securing property, cloud solutions for protecting against malware or for logging). Any conflicts between the requirements of data protection and information security must be resolved.

D3.2.3 Risk Assessment

It is the task of the controller and, if applicable, the processor to analyse and classify the identified risks for the data subjects. In doing so, the controller or processor must determine and document the severity and probability of occurrence of the identified risks according to objective standards. From this assessment, the respective level of risks follows on the basis of a risk function (e.g. in the form of a risk matrix) (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 protection needs of a natural person with regard to the processing of personal data in relation to his or her rights and freedoms result from the risk posed by the processing activity and its intensity of interference. The GDPR only knows the terms 'risk' and 'high risk', whereby 'risk' is referred to 'normal risk' . In addition, the GDPR uses the wording 'unlikely to result in a risk' (Art. 27 par. 2 lit. a) and Art. 33 para. 1 GDPR). Since there cannot be completely risk-free processing, the phrase 'not likely to result in a risk' is understood – based on its meaning and purpose – as 'only likely to result in a low risk' . Practical experience shows that there are such low risks that are not mentioned separately in the GDPR, but for which measures must also be taken. The measures for normal protection needs also cover such low risks.

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

- **No or low risk** of processing → **Normal need for protection** for persons affected by the processing
- **normal risk** of processing → n**ormal need for protection** for data subjects
- **high risk** of processing → **high need for protection** for data subjects

While the data subjects' protection needs as defined by the initial risk remain constant regarding the processing activity, the processing risks for the data subjects can be reduced by technical and organisational measures. These measures do not change the need for protection but reduce the risk of the processing activities. The initially present risks – the inital risks – must be reduced through process design and technical and organisational measures until a level of protection
appropriate to the risk (Art. 32 para. 1 GDPR) is achieved. In other words: The level of

12 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, as of: 26.04.2018, last accessed: 01/04/2019.

protection must be so high that the remaining residual risks of a processing operation can be justified by the controller. If there is no adequate residual risk, the processing activity may not be started due to a lack of legal compliance. If a 'high risk' and beyond remains, then Art. 36 GDPR provides that the controller must consult the competent data protection supervisory authority.

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

Due to the different objectives of the BSI's IT-Grundschutz (guaranteeing the information security of an organisation) and 'operational data protection' with the help of the SDM (guaranteeing the rights and freedoms of natural persons), it cannot be ruled out that the findings on the need of protection according to Grundschutz and according to SDM for the same processing will turn out differently. If the results of the assessment differ, then either the respective measures for the higher need of protection should be implemented or a more detailed analysis should be conducted to determine the reason for the different assessment results and how an appropriate 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 must be documented. Both in the case of an internal company or organisational evaluation or an audit or during a data protection audit, it must be comprehensible which concrete technical and organisational measures were 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 must be designed in such a way that, if possible, processing is carried out without reference to individuals or at least the risks are mitigated. 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 is to forego the automated retrieval procedure and implement a transfer in individual cases as a substitute.

When taking appropriate technical and organisational measures, the state of the art must be taken into account. The technical and organisational measures proposed in section D1 'Generic measures' are a good basis for developing appropriate measures for processing at a normal risk. In the future, these generic measures will be supplemented by the catalogue of reference measures. In the case of high risk, the following standardised strategy is recommended to effectively mitigate the risks.

1. The measures of the catalogue of reference measures must be implemented, which are to be taken in the case of normal initial risk of a processing or normal need for protection of a person.
2. Additional measures from the reference measures catalogue are to be implemented.
3. In addition, individual measures must be selected.
   An example of an individual measure could be the release of certain operations of a processing activity only upon request or after an examination and then to monitor this activity in operation so that a termination or the corrective measure is triggered in case of deviations.
4. The impact of a measure can be increased by using scaling options.
   An example of this is increasing the length of cryptographic keys used. Another example would be securing log data by operating a dedicated log server for processing log data, which stores all log data in a central location and prevents it from being accessed from the production machines and by their administrators.

5. Technical and organisational measures must 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 auditable by means of target/actual comparisons. Retroperspectivity means that log data must be generated, stored and processed. The log data must then be stored in an audit-proof manner through additional measures and its confidentiality must be guaranteed by transmitting and storing it signed and encrypted.

It should be noted that new risks may arise as a result of technical and organisational measures taken. These risks must be evaluated and appropriately reduced. As an example, a full logging of employee actions may be required, which at the same time carries the risk that an inadmissible control of performance and behaviour may take place through evaluations of this log. If, in this step, a processing operation is changed in such a way that the measures taken lead to new risks that are higher than the initial risk, and thus to an increase in the need for protection of affected persons, the design of the measures must be re-evaluated. The above strategies must 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 requirements of data protection law in an organisation. Data protection management in conjunction with the SDM is described in more detail below.

D4.1 Legal Basis for Data Protection Management

The controller is responsible for compliance with the principles for the processing of personal data and must be able to provide evidence of this. Specifically, according to Art. 30 GDPR, the controller must keep a catalogue listing the organisations' processing activities of personal data. In addition, he must already take appropriate technical and organisational measures at the time of determining the means (Art. 25 para. 1 GDPR – data protection by technical design). For processing activities that are likely to result in a high risk to the rights and freedoms of natural persons, they 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 result in a high risk and therefore requires 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 implemented on a permanent basis to ensure a level of protection appropriate to the risk for each 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 keep them up to date in this way.

In order for the controller to comply with the detailed requirements relating to the operational implementation of data subjects' rights and its accountability and verifiabillity obligations (cf. Section B1.8), a systematic approach to auditing and assessment is required, covering each individual processing activity as well as all personal processing activities of the entire organisation and the related technical and organisational measures. These accountability and verifiability obligations are a permanent task for the controller and should therefore be established as a permanent, cyclical process. The PDCA cycle (Plan, Do, Check, Act), known and proven from quality management, provides a continuous improvement process in four phases, which forms the basis for the data protection management process ((DSM process) described here.

The DPM process thus serves the controller in the systematic planning, ongoing operation, regular review of data protection compliance and improvement of processing activities (cf. B1.21 Evaluability). It thus creates transparency for the controller. The DPM process also helps the data protection supervisory authorities in advising controllers and in the data protection audits of these processing activities, as the data protection audits of the supervisory authorities usually correspond to this process flow.

D4.2 Preparations

Before starting the DSM cycle, the following three prerequisites must be clarified, just as before applying the SDM:[13]

13 Refer to fn. 5.

1. Clarity about the factual context in which the data processing under consideration 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.

To determine the factual circumstances at the Controller of the processing activity, the following questions, for example, must be answered:

- 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 is being processed, at what stage, and using what systems and networks?
- Which persons carry out the data processing and which persons carry out the monitoring?
- What ancillary processes are in place in support of the processing activity?

The legal basis for the processing must be determined as part of the assessment of the lawfulness of the processing. 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 carried out in the public interest or in the exercise of official powers vested in the controller?
- Is the processing necessary for compliance with a legal obligation to which the controller is subject?
- Is the processing necessary to protect the vital interests of the data subject or 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 authority vested in the controller?
- Is the processing necessary for the purposes of the legitimate interests of the controller or a third party? Does this override the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, especially if the data subject is a child?

The legal analysis provides clarity on how – based on Art. 5 of the GDPR – personal data may be processed. It starts with an examination of the lawfulness of the processing.
In addition, it provides answers to the following questions in particular, which prepare the application of the SDM:

- Which national law is applicable to the processing?
- What legitimate purposes can be pursued with the processing and what changes of purpose are permissible in the course of the processing?

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 data are relevant and necessary for the fulfilment of the legitimate 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 regulated (Art. 28 GDPR)?
- What are the specific requirements to be met by the technical and organisational measures in relation to the individual case?

The comprehensiveness and level of detail, especially of the findings on the factual relationships, will vary from processing to processing, as will the degree of formalisation of the procedure, from informal questioning to the use of standardised questionnaires. Regardless of this, a structured summary of the results is as common as it is indispensable for the further steps. The findings on the factual context are included in phase 1 'Plan/Specify/DSFA' of the DSM 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 to determine how the protection goals for the data processing under consideration are operationalised. Depending on the identified risk (see also section D3) and with reference to the specific legal requirements, the characteristics of the processing activity resulting from the respective assurance objectives must be determined in more detail in qualitative terms:

- **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 benchmark for the concretisation of the protection objective of availability is the influence of the possibility of proper use of the data in the interest of the data subject.
- **Integrity** *Which data is related to an identified or identifiable person and must therefore be kept intact and up to date? How is it ensured that processes, systems and services are correctly planned, operated and controlled in accordance with the set purpose?* Again, the interests of the data subjects are the benchmark.
- **Confidentiality** *Who is to be denied access to which data? Which processes, systems and services are potentially vulnerable to unauthorised access?* The extent of authorised access must first be derived from the respective business processes, independent of technology. This determines the framework within which the measures for confidentiality protection against unauthorised employees of the responsible party must operate. 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 is data processing to be kept transparent vis-à-vis data subjects and supervisory authorities?* The requirements for information and disclosure obligations pursuant to Art. 12 et seq. GDPR, the notification obligation pursuant to Art. 34 GDPR, the documentation of processing pursuant to Art. 30GDPR, the internal documentation of processing operations and their evaluability as well as the revisability of processing must be specified.
- **Intervenability** *To what extent are data subject rights to be granted?* It must be specified how data subjects can exercise their rights, how it is ensured that requests are justified, how the processing of personal data can be intervened in (e.g. by rectifying, erasing or restricting the processing of personal data) and in what form data can be transferred from or to other controllers.
- **Unlinkability** *What changes of purpose are permissible? What purposes of anciliary processes are legitimately derived from the 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 minimisatio**n *In what way is the requirement of data minimisation implemented?* It must be clarified how the knowledge of and the exercise of which power of disposal over which data of the data subjects by which persons and bodies are to be minimised. This also includes setting retention periods for personal data as well as processes to ensure compliance. The starting point is again the interests of the data subjects to limit the burden to what is necessary, even within processing for legitimate purposes.
- **Resilience** *Are systems and processes adequately prepared for events that cause disruptions to regular operations*? It must be clarified which damaging events, disruptions or attacks could have a negative impact on those affected and whether countermeasures are available for this and whether they can be applied in a targeted and timely manner. Due to the cross-sectional nature of the resilience objective, 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 assurance objectives.

Once the performance objectives have been qualitatively specified with regard to the processing activity, technical and organisational measures can be determined. For this purpose, the results of the data protection impact assessment are used, if one has been carried out. The risk to the rights and freedoms of data subjects identified in the risk assessment is decisive for further action. The result of the risk assessment is taken into account in three ways.

Firstly, the protection goals can be quantified in more detail. Examples of clarifications are answers to the following questions: For what period of time is the loss of data availability tolerable for those affected, and to what degree? With what delay should 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 for which 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 result of the data protection impact assessment flows into the evaluation of the residual risks that remain after implementation of the measures that can be taken with an effort that is proportionate to the purpose of the processing. These risks may be the result of the interests of third parties or participants that are contrary to the protection goals, such as unauthorised access to the data subject's data, processing for unlawful purposes, processing beyond what is necessary or processing 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 the threshold analysis and data protection impact assessment and the resulting selection of a set of technical and organisational measures (target values) by matching 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 are 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 ongoing operation (**phase 3a**). This is followed by an assessment of compliance with the legal requirements and any remaining risks to the rights and freedoms of the data subjects (**phase 3b**). If the level of protection is too low or the residual risks are judged to be too high, they must then be reduced to an acceptable level through appropriate improvements, for example through additional measures (**phase 4**).

The assessment made at the end of phase 3 can subsequently form the basis for the recommendation or request of the supervisory authority as well as the instructions for the Controller to either remedy the deficits through additional technical or organisational measures or to refrain from the processing activity insofar as legal compliance cannot be

established or sufficient risk reduction cannot be achieved by proportionate means (phase 4 of the DPM cycle).

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

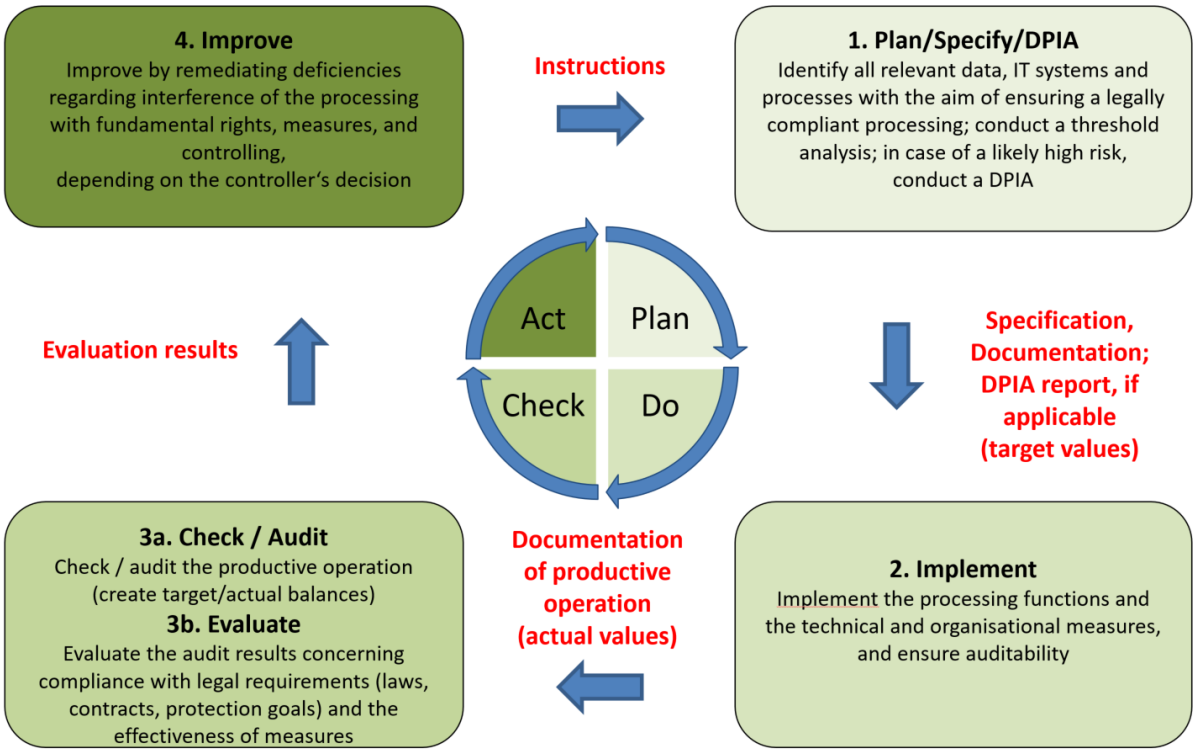

Figure 1: The PDCA data protection management cycle (DPM cycle) as a framework for the application of the standard data protection model in planning, consulting and audit processes

For each processing activity, it will usually be necessary to go through the DPM cycle several times. This particularly applies to the Controller when planning processing activities. For example, when a specialised procedure is put into operation, a first cycle could concern its test operation, the second cycle the pilot operation and the third cycle the 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 in the context of an audit process by the supervisory authority.

D4.4.1 Plan: Specify / DPIA / Documenting

Phase 1 identifies appropriate measures to mitigate the risks of interference with fundamental rights, to ensure the protection of personal data and to demonstrate compliance with the Regulation when planning a processing activity involving individuals. To provide evidence of the effectiveness of the measures, functional requirements (target values) must be defined and documented. These are derived from the legal requirements (target) (see Part B Requirements of the GDPR). It is only then that it is determined which

activities of the programmes and systems and which events of the processes are to be recorded.

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

A DPIA must be carried out if the form of processing, especially when using new technologies, is likely to result in a high risk due to the nature, scope, context and purposes of the processing. Whether a processing activity involving individuals is likely to result in a high risk must be determined in advance within the framework 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 its context 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 DPM.

Further details on the systematic implementation of a data protection impact assessment can be found in Short Paper No. 5 of the Data Protection Conference.[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 target values, activities of IT systems and administrators and other relevant events are documented and logged in an auditable manner. If a DPIA report is available, the Controller must take its results into account when implementing processing activities.

During the implementation of systems and programmes, it must be ensured that system documents and protocols can be used to verify the functions of specialised applications and

16 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, Stand: 26.04.2018, last accessed: 01/04/2019.

the security of IT systems and services at the various levels (e.g. client, server).
The availability of these documents and logs (actual values) is a prerequisite for the performance of phase 3 of the DPM.

D4.4.3 Check: Check / validate / evaluate

Correlating the functional target values determined in the planning phase with the actual values determined (phase 3a) is the core application of SDM in the DPM cycle. In addition, the relevant reference measures are compared with the technical and organisational measures actually implemented. Deviations from the objective must be assessed in terms of their impact on the implementation of the principles of Art. 5 of the GDPR or the achievement of the protection goals. In the event of an audit by the supervisory authority, the analysis carried out up to this point allows the conclusion to be drawn from a failure to meet performance targets to (possibly sanctionable) data protection deficiencies.

In audit and assessment practice, it can often be determined with little effort whether requirements have not been met because the associated actions are not in place, the actions have been implemented incorrectly or inadequately, or the reference actions have not been applied correctly. The case is more complicated if the body to be audited has chosen measures other than those in the catalogue of reference measures. Even if these can be judged to be suitable in principle, a separate assessment must be made of whether they actually address the identified risk in their specific design. 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 assessment phase (phase 3b), these differences are translated into legal terms and compared with the data protection requirements (target). Un the context of a data protection assessment, the identified deviations may become ‘normative deficiencies’. The more serious the deficiency, the more effectively it needs to be addressed through appropriate change instructions in Phase 4 of the DPM process. This will require a repeat of all phases of the DPM cycle. The outcome of Phase 3b consists of assessments that are appropriate to bring 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 subsequently be taken. These assessments will be the outcome of phase 3 and will be the subject of discussion and prioritisation by the Controller in phase 4. In this Phase 4, identified deficiencies must lead to decisions by the Controller and resulting instructions to change or create new actions, which must then be planned, implemented and tested in a new cycle. If measures have been taken that eliminate all deficiencies, it can be

assumed that all deficiencies have been eliminated and the processing activity is legally compliant.

Part E: Organisational Framework

E1 Interaction of SDM and BSI Grundschutz

The SDM is closely related to the Grundschutz methodology of the Federal Office for Information Security (BSI). The IT-Grundschutz developed by the BSI makes it possible to identify and implement necessary security measures through a systematic approach. The BSI standards provide proven procedures for this, and the IT-Grundschutz compendium provides tangible requirements. When selecting measures, the basic protection is primarily oriented towards the protection goals of availability, , integrityand confidentiality known from IT security..

In order to facilitate the application of SDM, the SDM methodology uses modelling mechanisms that are comparable to those of the Grundschutz methodology. BSI-Grundschutz and SDM are based on the same modelling of a processing activity. SDM also comprehensively considers the components of personal data by modelling the processing activity (business process) with its components, systems and services, and sub-processes. 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 of data subjects is determined from this risk and also divided into three levels. A direct connection is made between the risk (level) and the need for protection (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. However, the objectives of BSI-Grundschutz and SDM differ significantly. When selecting suitable technical and organisational measures, SDM takes the perspective of the data subject and his or her exercise of fundamental rights and therefore differs from the perspective of IT-Grundschutz. IT-Grundschutz focuses primarily on information security and is intended to protect the institution processing the data. For the selection of measures according to the SDM, on the other hand, the impairment that a data subject must accept due to the institution's data processing is decisive. Against this background, a distinction must be made between the selection of measures to ensure information security for institutions by responsible bodies and that of measures to ensure 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 reference to data protection from which – as in the area of IT security – technical and organisational measures are derived. In this sense, the protection goals of data protection require a somewhat broader understanding compared to the protection goals of IT security, because data protection additionally takes a broader, extended protection perspective by also considering the risks posed to the rights and

freedoms of natural persons by the activities of the organisation itself within and outside its business processes.

As part of the BSI's modernisation of the basic protection methodology, the relationship between data protection and information security has been 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 of data subjects. The new Grundschutz Compendium, which replaces the Grundschutz Catalogues, contains in the section 'CON: Concept and measures' the new module 'CON.2 Data protection', which describes the demarcation between information security and data protection. The requirement 'CON.2.A1 Implementation of standard data protection model' states 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 together provide the information required to demonstrate compliance with the principles for 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 clarifying who is responsible for the SDM, which version is currently valid and at what time which version was valid and where this current version can be obtained. The operational concept regulates three aspects:

- Clarification of roles and responsibilities in relation to the model,
- Ensuring the applicability of the SDM,
- Creating transparency with regard to the publication and further development of the model.

E2.2 Contractor, Project Management, User

The Contractor for the development and maintenance of the SDM are the members of the Conference of Independent Data Protection Authorities of the Federation and the Länder (Data Protection Conference – DSK). The DSK owns and publishes the SDM, which includes both the methodology and the catalogue of reference measures.

The development and maintenance of the SDM is carried out by the working group 'Technische und organisatorische Datenschutzfragen'(Technical and Organisational Data Protection Issues) of the DSK (AK Technik). The AK Technik is responsible for project management.

The SDM can be used both by the sixteen State Data Protection Commissioners, the Bavarian State Office for Data Protection Supervision as well as the Federal Data Protection Commissioner within the framework of their legal advisory, verification and sanctioning activities (*user group 1*) and by controllers and processors for the planning and operation of the processing of personal data as well as data protection officers within the scope of their advisory and auditing activities (*user group 2*).

The model will be further developed both in the context of the practice evaluation and in accordance with professional requirements as follows:

- Preparation 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 submitted 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, which includes
    - Provision of a Single Point Of Contact (Service Desk);
    - Operation of CR tracking;
    - Moderation of discussions;
    - Managing the necessary resources (website, project platform);
- Public relations.

E3 Changes in the different SDM versions

E3.1 Changes from V2.0 to V3.0 (as of 01. November, 2022)

Section D2.1 'Breakdown of a processing activity into operations or into phases of a data life cycle': To be able to analyse or design a processing of personal data, appropriate methodological tools are required. Section D2.1 proposes 9 groups of processing operations to summarise the (at least) 14 elementary processing operations mentioned in the GDPR. Alternatively, an even more compact life cycle model consisting of 4 phases is presented. Elementary processing operations have been assigned to groups or phases if the data protection requirements for them are similar according to experience. The groups or phases can then be used if this is appropriate to the problem in the respective individual case.

Section D2.5 'Overview of SDM modelling techniques ("SDM cube")': This section shows the relationship of the systematics introduced in sections D2.1, D2.2 and D2.4 to each other. It is usually necessary to analyse personal data processing operations according to all three of these aspects. However, the classifications are independent of each other. Each combination of (elementary) processing operation, protection goal and (technical) component may present a specific risk to the rights and freedoms of natural persons, which requires a

specific set of measures. The ‘SDM cube’" is therefore a meaningful overall picture of the risks of processing activities.

The amendments in sections D2.1 and D2.5 are closely related in terms of content.

Section D3 ‘Risks and Need for Protection’:T The GDPR has brought the aspect of ‘risk’ to the rights and freedoms of a processing operation to the fore. The concept of the need for protection, as used in BSI-Grundschutz, was emphasised at the beginning of the work on the SDM. Therefore, the text as a whole, and especially Chapter D3, had to be revised in this respect. In addition, four risk types were added to section D3.1 ‘Risks for data subjects’. This typology has the same wording in the current draft of the IT-Grundschutz "CON.2 - Data Protection’ module and it is desirable that IT-Grundschutz and SDM, with mutual references, can explicitly fall back on a common anchor for understanding data protection risks.

Further changes concern improvements to the consistency of content and the quality of language.

E3.2 Changes from V1.1 to V2.0 (as of 5.11.2019)

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

Part A describes the purpose, scope and structure of the model, the content of which has not changed since the previous version. The SDM includes seven protection goals, a strategy for grading risks or protection needs, and the three functional components of a processing activity. What is new is that the ‘services’ mentioned in the GDPR supplement the ‘IT systems’.

Compared to the previous version, Part B aligns the SDM V2.0 even more closely with the requirements of the GDPR. In particular, all individual concrete measures mentioned in the GDPR for the implementation of data subjects' rights are taken into account. Furthermore, a chapter on ‘Consent Management’ and ‘Implementation of Supervisory Authority Orders’ has been added.

In Part C, the protection goals are assigned to the principles of Art. 5 GDPR as before, as well as to the many individual legal requirements from Part B. The SDM 2.0 thus ensures the implementation of the data subjects' rights. The SDM 2.0 thus ensures the complete consideration of operational requirements of the GDPR much better than before. This chapter replaces the mapping of protection goals and articles of the GDPR from SDM-V1.1/p. 21, Table 1 and 2.

Part D presents the practical implementation; this is where the biggest changes were made compared to the previous version. In the chapter on 'Risk and Need for Protection', the conceptual innovation compared to V1.1 is a clear presentation of the relationship between need for protection and risks: The need for protection of a person arises from the risks that a processing activity involving a person would generate without technical and organisational measures. While the need for protection of data subjects determined in this way remains constant, the risks can be reduced – through the design of the processing activity as well as through the operation of technical and organisational measures; this reduction must take place down 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 concise presentation of a Deming cycle specifically adapted to data protection audit requirements. The conceptual innovation is to show the exact location of the mutual reference of the target/actual audit processes, which concern technical and organisational targets, and the evaluation of normative target/actual assessments. Each of the four phases generates products (specifications, documentation, assessments, instructions from the responsible person) as an output, which in each case forms the input of the subsequent phase. This chapter takes many aspects from chapter SDM-V1.1/p. 34, 'Testing and consulting' and replaces them.

Special attention has been paid to a more consistent use of the term 'processing activity' (formerly 'procedure'), which is a central aspect 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, 'processing activity' is now used as the generic term, with 'processing operations' (such as collecting, storing, querying) as components. The term 'processing operation' can also be used to refer to such sub-processes of a processing activity.

E3.3 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.

Chapter 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

[empty]

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 in the concrete context, 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.