The Standard Data Protection Model

A concept for inspection and consultation on the basis of unified protection goals

V.1.0 – Trial version

Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

Content

Preface to the Translation

The Standard Data Protection Model (SDM) sets the stage on which legal requirements and the selection and implementation of technical and organisational data protection measures systematically interrelate. Thereby, on the one hand, allowing Data Protection Authorities to conduct more transparent and upright reviews of technical and organisational data protection measures. On the other hand, the SDM provides a methodology for assessing the efficacy of data protection measures required by data protection regulations. But likewise the SDM addresses controllers and processors regarding the planning, implementation and supervision of data protection measures and functions.

In November 2016, the Conference of the Independent Data Protection Authorities of the Bund and the Länder authorised the SDM for publication. The Conference recommends the evaluation of the SDM. Please note, that the text at hand is only a *literal translation* of the SDM guideline. An international version of this text is currently being prepared.

The SDM embraces the legal requirements set by the GDPR which came into force in May 2016. Nevertheless, this version is also referring to German regulations applicable until May 2018. The next English version will focus even more closely on the aspects of the operationalisation of fundamental rights by an appropriate selection and implementation of organisational measures and technical functionalities. The authors are aware that the references to national legal specifics still included in the text at hand are not relevant in international contexts, but have nevertheless decided to already provide this version to an international audience to open a forum for discussion and enabling immediate feedback.

The authors would also like to mention that SDM does not only offer a methodology, but a *specific* set of data protection measures that are compiled in a catalogue which specifies the data protections measures listed in chapter 7 of this guideline and which is available in a draft version since October 2016. This catalogue, consisting of individual sets, is currently undergoing an annotation phase among the German Data Protection Authorities and therefore has not yet been published. Completed sets will be gradually released, translated, and published on the websites of the German Data Protection Authorities.

Any comments to further clarify and improve the SDM are encouraged and welcomed.

The authors

Schwerin in March 2017

1 Introduction

The European General Data Protection Regulation 2016/679/EC (GDPR) came into force on May 25, 2016 and will apply in all European Union Member States from 25 May 2018. The GDPR lays down rules for the protection of natural persons with regard to the processing of personal data and protects the fundamental rights and freedom of natural persons, in particular their right to the protection of personal data. Articles 5, 12, 25 and 32 provide essential requirements on the security of the processing of personal data. The regulation calls for appropriate technical and organisational measures to guarantee a level of protection appropriate to the risk (Article 32 (1)). In addition, the GDPR requires a procedure for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures (Article 32 (1) (d)). The GDPR provides the possibility to assess IT-based procedures in codes of conduct and by certification mechanisms (Articles 40-43 GDPR). Finally, the GDPR introduces a consistency mechanism that integrates the independent supervisory bodies in a complex consultation procedure (Chapter VII–Cooperation and Consistency). This procedure requires a coordinated, transparent, consistent, and plausible system to assess the processing of personal data with regard to data protection.

Article 5 GDPR sets out basic principles for the processing of personal data: Personal data shall be processed lawfully, fairly and transparently, collected for specified, explicit and legitimate purposes, based on accurate data, protected against loss, destruction or damage and in a way that ensures their integrity and confidentiality. The *Standard Data Protection Model* (SDM) provides appropriate mechanisms to transfer these regulatory requirements of the GDPR into technical and organisational measures. In order to achieve this purpose, the SDM structures the legal requirements in terms of data protection goals like data minimisation, availability, integrity, confidentiality, transparency, unlinkability, and intervenability. The SDM uses these data protection goals to transfer the legal requirements of the GDPR into a catalogue of technical and organisational measures, which the regulation itself requires. With this reference catalogue of data protection measures it is possible to review the effectiveness of the measures. Such standardised catalogues of measures further provide a well-suited basis for the specific data protection certifications promoted by the GDPR.

Data protection standardisation therefore also supports the cooperation of supervisory authorities, as stipulated in the regulation. German data protection authorities must increasingly cooperate and monitor modern procedures for the automatic processing of personal data with coherent concepts for consultation and investigation. The SDM as a holistic consultation and investigation concept can lead to a harmonised, transparent and plausible system of 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. On October 18, 2015, the IT-Planning Council decided to further develop the NEGS. In the NEGS, the Bund, the Länder and the local municipalities agreed on the future development of electronic pro-

cessing of administrative matters over the internet. One of the central principles guiding the Bund and the Länder in their joint as well as in their individual actions concerning e-government relates to questions of information security and data protection. The NEGS stresses that e-government must be secure and in compliance with data protection principles if it wants to achieve and retain the unconditional trust of citizens and businesses in electronic administrative management. In order to guarantee the protection of personal data technical and organisational measures which respect the principle of data minimisation and relate to the data protection goals of availability, confidentiality, integrity, transparency, unlinkability and intervenability are demanded. The SDM is based on these objectives and is an excellent tool to implement the NEGS data protection objectives.

The Standard Data Protection Model as described here can contribute substantially to a fundamental rights-based enforcement of data protection in Germany as well as on a European level and applies to the private and the public sector. On the one hand, the SDM provides a systematic and verifiable comparison between nominal or target specifications derived from regulations, standards, contracts, declarations of consent and organisational rules, and, on the other hand, the implementation of these specifications both at the organisational and technical level in IT-based procedures and systems.

The SDM provides *one* method to eliminate or at least reduce the risks to the right to informational self-determination, which are necessarily associated with 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 development of data protection and data security concepts. New methods which are comparable to the SDM but are modified in details result from these experiences and are often used to minimise the risk. These methods can, of course, have their merits in specific application contexts.

The SDM was developed by the supervisory authorities in a phase of change in European data protection law. The GDPR came into force on 25 May 2016, but will be applicable only after a transitional period of two years. During this transitional period, national data protection regulations such as the German Federal Data Protection Act (BDSG) or the data protection laws of the Länder apply without restriction. In order to facilitate the application of the SDM even during this transitional period, the following text is based not only on the GDPR, but also deliberately refers to the German Federal Data Protection Act. At the end of the transitional period in May 2018, the SDM will be revised with regard to the then applicable legal bases.

2 Purpose of the Standard Data Protection Model

Under data protection law, it has to be assessed whether the processing of personal data by means of IT-based procedures is based on an appropriate legal basis. The processing of personal data is generally prohibited by Section 4 (1) of the German Data Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), the corresponding provisions of the data protection laws of the Länder and, in future, Article 6 (1) GDPR. The latter contains principles for the processing in its Article 5 and the conditions for the lawfulness of the processing in Article 6. Further, it has to be ensured that the data is processed with an appropriate selection of technical and organisational measures in order to protect the rights of the data subjects (see Annex to Section 9 BDSG or, in the future, especially the principles for the processing pursuant to Article 5 GDPR and the rules on the safety of processing under Article 32). The SDM described here systematises these measures on the basis of protection goals.

The model is, on the one hand, directed at controllers who are enabled through recourse to the SDM, to systematically plan, implement and continuously monitor the necessary functions and protection measures. On the other hand, the model is also aimed at supervisory authorities and enables them to reach a transparent and plausible, reliable judgment on a procedure and its components.

The starting point of the analysis is the determination of the controller or controllers as well as the purpose of the processing in the context of a business process, which is implemented or supported by the procedure, and the relevant legal bases. Only when these legal prerequisites have been attained, it is feasible to specify the functionality of the procedure including the necessary scope of the processing of personal data and the appropriate data protection measures with regard to the state of the art.

3 Scope of Application of the Standard Data Protection Model

The major application of the Standard Data Protection Model is the planning, implementation and operation of individual procedures involving the processing of personal data (personenbezogene Verfahren) and its evaluation by the supervisory authorities. Such procedures are characterised by the fact that they relate to a specific, distinct and lawful processing purpose (in the public sector a legal basis for processing) and to the business processes implementing this purpose (see Chapter 8).

The data protection laws of the Bund and the Länder require the selection and implementation of technical and organisational measures – which are necessary and appropriate according to the state of the art and the protection of the data to be processed – for every processing of personal data. These data protection measures are considered part of the procedure, including any potential processing of personal data within its context.

The legal basis may prescribe specific measures which are to be implemented procedure-specific, such as the anonymisation of collected personal data once a certain purpose of the processing has been achieved. There may also be cases where particular measures have to be taken as a result of a balancing of interests required by law.

In both cases, further measures, which are used across multiple procedures, complement these procedure-specific data protection measures. These more general measures can, for example, be aimed at the encryption of data, the assurance of the integrity of data, the authentication of communication partners and technical components, the logging, the pseudonymisation and anonymisation or the handling of contact addresses for complaints, or they offer a general framework for role concepts in different procedures in general.

The SDM aims at systematising mandatory as well as optional, procedural as well as cross-procedural data protection measures and facilitating their respective assessment.

The SDM can be used by the sixteen national data protection commissioners, the Bavarian Data Protection Authority, the Federal Data Protection Commissioner, as well as by controllers for the planning and operation of procedures for the processing of personal data.

4 Structure of the Standard Data Protection Model

The Standard Data Protection Model:

- Transfers legal data protection requirements into a catalogue of protection goals,
- Structures the procedures under consideration into the components data, IT-systems and processes,
- Incorporates the classification of data in three tiers of protection levels,
- Complements these with considerations on the level of procedures and IT-systems and
- Provides a systematically derived catalogue of standardised data protection measures, which have been systematically derived from these principles (see Annex).

5 Data Protection Goals

5.1 The Term 'Data Protection Goals'

The SDM uses the term 'data protection goals' to describe certain categories of requirements derived from data protection law. These requirements are aimed at properties of lawful processing operations, which have to be ensured by technical and organisational measures. This is ensured through the exclusion of deviations. For instance, one of the attributes of lawful processing is that it does not lead to unauthorised knowledge of the data. The measures must thus aim to exclude any possibility of unauthorised knowledge of the data. The level of realisation must be determined through a balancing of the level of protection (see Chapter 8) and the expenses taking into regard the state of the art. The obligation to implement the protection goals through technical and organisational measures is thus not to be regarded as absolute, but must always be regarded in the context of the specific circumstances of the processing and the associated risks for the rights and freedoms of the data subjects.

The term 'data protection goal' (Gewährleistungsziel) is particularly appropriate to establish a reference to the ruling of the German Federal Constitutional Court in 2008 (Judgement of 27 February 2008 – 1 BvR 370/07, 1 BvR 595/07, Official Record of Decisions [BVerfGE] 120, 274). In this judgement, the Federal Constitutional Court educed and explained the fundamental right to ensure confidentiality and integrity of information technology systems (see also Chapter 6.1).

Finally, the choice of this term aims to counter the impression that the catalogues of protection goals which are already included in some of the data protection regulations of the Länder are expanded without the legitimatisation of the legislator.

5.2 The key legal requirements for data protection

The following legal data protection requirements, which are laid down in all German data protection laws and which have to be met in order to process personal data lawfully, are captured by the concept of protection goals:

- The purpose limitation principle,
- The limitation of data processing to the extent necessary with regard to data avoidance,
- The consideration of the rights of the data subjects, which require that procedures include processes to inform the data subject, rectify, block and erase personal data,
- The transparency of procedures as a prerequisite to ensure that the legal requirements are met, which should be verifiable both for the organisation itself and, at least in a generally comprehensible way, for the data subjects as well as for the supervisory authorities,
- The information security of components used for data processing.

The SDM does not consider fundamental questions of the substantive lawfulness of a process or any sector-specific regulations or provisions at a high level of detail (see point 10). The focus on the generally applicable data protection goals therefore does not render the cognisance of the data protection regulations unnecessary, not even in the area of technical and organisational measures.

5.3 The Fundamental Protection Goal of Data Minimisation

It is a common trait of all protection goals that they determine in advance which properties and parameters of processing operations and support processes are permissible. For this reason, the legislator calls for the limitation of the data to the essential and to a necessary extent (Article 5 (c) GDPR), at the source and at each branch, in advance and – increasingly important in the age of explorative data processing linked to the buzzword *Big Data* – to the processing itself. This basic requirement concisely captures the objective of data minimisation. Its implementation has a sweeping effect on the scope and level of the protection programme defined by the other protection goals.

Data minimisation substantiates and operationalises the principle of necessity, which requires from any process as a whole as well as any of its steps not to collect, process and use more personal data than necessary for the achievement of the purpose of the processing. Data minimisation is to be taken into account proactively as an element of data protection-friendly design. Starting with the design of information technology by the manufacturer and its configuration and adaptation to the operating conditions, to its use in the core and auxiliary processes of the operation, for instance in the maintenance of the systems used; from the collection of personal data, through its processing and use, to its erasure or complete anonymisation; throughout the entire life cycle of the data.

The attainment of this protection goal presupposes that the appropriateness and legitimacy of the purpose, as well as the relevance or necessity of the data to be collected for these purposes. This occurs on an abstract level, without consideration of procedural and technical constraints. It may lead to the conclusion that the processing of personal data is not necessary and that consequently, the data may not be processed. By realization of such data avoidance, the optimal data minimisation is achieved.

If complete data avoidance is not possible, sequences of processing steps can be evaluated on the basis of the legitimate purpose and data basis:

- According to the extent of information processed or disclosed,
- According to the number of entities and persons to whom this information is disclosed, and
- According to the extent of the factual control which the respective entities and persons exercise over the data.

The protection goal of data minimisation is achieved when the processing in these three dimensions is minimised globally throughout the entire processing operation and, within its

framework, locally in each and every individual processing step. Obvious examples of parameters that allow minimisation are data fields in search masks and interfaces or functions that are offered to users in menu-driven systems.

The principle of data minimisation assumes that optimal data protection is achieved when no or as little personal data as possible are processed. Data minimisation as a protection goal is achieved when an appropriate approximation of this optimal state is achieved. This optimisation objective is based on the evaluation criterion of minimising the factual control and knowledge in the three dimensions listed above. Based on this principle, the optimal series of steps in the processing can be chosen, and, as a result, it can be adapted to changing conditions. In the course of processing, it must be ensured through recourse to technical and organisational measures that data processing is only carried out within the predefined framework.

The earliest possible time of erasure of personal data that are no longer required is one such measure, certainly the most important and most effective. Prior to this, however, individual data fields or attributes may be excluded from certain forms of processing, or the number of data sets to which a functionality is applied can be restricted. Data fields which enable the identification of data subjects can be erased or transformed (anonymisation, pseudonymisation). Alternatively, their visibility in data masks can be suppressed so that the actors are not aware of their existence or contents, provided this knowledge is dispensable for the processing purpose.

5.4 The Fundamental Protection Goals

5.4.1 The Classic Protection Goals of Data Security

Since the end of the 1980s, protection goals have played a part in the design of technical systems, whose safety is to be ensured. The '*classic' protection goals in data security* are:

1. Availability,
2. Integrity, and
3. Confidentiality.

(1) The protection goal of *availability* is the requirement that personal data must be available and can be used properly in the intended process. Thus, the data must be accessible to authorised parties and the methods intended for their processing must be applied. This presupposes that the methods can deal with the available data formats. Availability comprises the ability to find specific data (e. g. by means of address directories, reference or file numbers), the ability of the employed technical systems to make data accessible to individuals in an adequate manner, and the possibility to interpret the content of the data (semantic ascertainability).

(2) 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

have been determined for the execution of their intended functions. On the other hand, integrity means that the data to be processed remain intact, complete, and up-to-date. Deviations from these properties must be excluded or at least ascertainable so that this can either be taken into consideration or the data can be corrected. If the protection goal integrity is understood as a form of accuracy within the meaning of Article 5 (1) (d) GDPR, this leads to the claim that there is sufficient congruency between the legal-normative requirement and common practice, both in terms of technical detail as well as in the broad context of the procedure and its overall purpose.

(3) The protection goal of *confidentiality* refers to the requirement that no person is allowed to access personal data without authorisation. A person is not only unauthorised when it is a third party external to the controller, regardless of whether they act with or without a criminal intent, but also employees of technical service providers who do not need access to personal data for the provision of the service, or persons in organisational units who are unrelated to the respective procedure or data subject.

Over the last years, these three protection goals have been increasingly taken into consideration by controllers in their own interest, even without any legal requirements. Initially, they were formulated exclusively for IT security and describe requirements for secure operation, in particular the operation of procedures of organisations with regard to their business processes. Organisations have to protect their business processes from attacks regardless of whether they are carried out by external or internal persons.

5.4.2 Protection Goals Aimed at the Protection of Data Subjects

In addition to the protection goals of IT security, further data protection-specific protection goals have been derived from existing data protection regulations. In turn, technical and organisational measures can be derived from these protection goals. From a data protection point of view, organisations must also protect their business processes against attacks when personal data are affected by these business processes. In this respect, the protection goals of data protection require a broader understanding compared to the IT security protection goals, as data protection also takes on an extended perspective for protection by regarding the risks arising from the activities of the organisation itself for the data subjects within and outside of their business processes. Methodically speaking, it is not only a person who has to prove trustworthy to an organisation through verifiable characteristics, but an organisation also has to prove that it is trustworthy to the person. A Data Protection Impact Assessment (Article 35 GDPR) is particularly suited to demonstrate this fact.

The following protection goals of data protection, which are aimed at the specific protection requirements of data subjects, reflect the data protection requirements in an operational form:

4. Unlinkability,
5. Transparency, and
6. Intervenability.

(4) The protection goal of *unlinkability* refers to the requirement that data shall be processed and analysed only for the purpose for which they were collected.

Data sets can in principle be processed for further purposes and can be combined with other, potentially publicly available data. Larger and more meaningful data sets also increase the potential for abuse, i.e. to use the data unlawfully, for purposes beyond the legal basis. Such further processing is lawful only in strictly defined circumstances. The GDPR only allows them to be used for archival purposes which are in the public interest, for scientific or historical research purposes or for statistical purposes, and explicitly calls for safeguards for the rights and freedoms of the data subjects. These safeguards are to be achieved through technical and organisational measures. In addition to measures of data minimisation and pseudonymisation, other measures that allow the further processing to be separated from the source processing are also suitable, ensuring separation both on the organisational and on the system side. The data base can, for example, be adapted to the new purpose by pseudonymisation or reduction of data volume.

5) The protection goal of *transparency* refers to the requirement that the data subject as well as the system operators and the competent supervisory authorities must be able to understand, to a varying extent, which data are collected and processed for a particular purpose, which systems and processes are used for this purpose, where the data flow for which purpose, and who is legally responsible 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 origin to their erasure and is a prerequisite for lawful data processing. Informed consent, where it is necessary, can be given by data subjects only if these criteria are met. Transparency of the entire data processing operation and of the parties involved can help ensure that data subjects and supervisory authorities can identify deficiencies and, if necessary, demand appropriate procedural changes.

(6) The protection goal of *intervenability* refers to the requirement that data subjects are effectively granted their rights to notification, information, rectification, blocking and erasure at any time, and that the controller is obliged to implement the appropriate measures. For this purpose, controllers must be able to intervene in the processing of data throughout the process; from the collection to the erasure of the data.

5.5 Further Derived Protection Goals

Some data protection laws of the Länder use further protection goals that are not listed among the fundamental protection goals of the SDM. However, they can be derived from the above-mentioned fundamental protection goals. Some of these derived protection goals will be highlighted in the following.

The protection goal of *authenticity* refers to the requirement that personal data can be traced unambiguously to their origin.

Depending on the nature of the data's origin, different information must be retained and the link of the data with this information must be secured: In instances of collection of data from data subjects themselves, this information includes the collection process, its date of expiry and, where appropriate, the identity of the person collecting the data; in the case of the data transfers or the retrieval of data sets from third parties, this includes the point in time, the occasion and purpose of the transfer or retrieval, as well as the data source; in the event of an adoption of a data set leading to a change in purpose, the name and revision level of the source data set and a reference to its documentation must be included.

This protection goal is derived from the comprehensive protection goal of transparency. It can only be achieved by ensuring the integrity of the link between data and their source, and can thus also be understood as a form of "integrity-assured transparency".

The protection goal of *revisability* describes the requirement that it must be possible to monitor who processes personal data at what time and in what manner. It monitors editing of the data as well as the use and mere perusal of data. This protection goal forms part of the broader protection goal of transparency and can only be achieved by maintaining the integrity of the link between the data set and the information about to the processing.

6 The Connection of Protection Goals with Existing Data Protection Law

Legislation cannot be readily operationalised in a technical manner. Lawyers and computer scientists must therefore find a common language to ensure that the legal requirements are actually implemented technically. The protection goals supports them in doing so, as data protection requirements can be assigned to individual protection goals according to their importance, their intended effect, and their objective and thus be bundled in a structured manner. The technical design of systems can be based on these practicability aimed objectives, so that data protection requirements can be transformed into the required technical and organisational measures via the protection goals.

6.1 Protection Goals in the Jurisdiction of the Federal Constitutional Court

The protection goals only address claims that are covered by law. They ultimately correspond with the basic principles for safeguarding the right to informational self-determination (see section 5.2), as established in the census decision (BVerfG, ruling of 15 December, 1983, 1 BvR 209/83 et al.). The BVerfG pointed out that the free development of personality under modern conditions of data processing requires the individual to be protected against the unlimited collection, storage, usage, and transfer of his or her personal data. Considering the possibilities of processing and linking inherent in information technology, the BVerfG had referred to the protection of the data subjects against the misuse of the data processing purpose. Focusing on transparency for the data subjects and their self-determination enables them to understand what personal information is known, so they are able to plan and decide self-determined.

In addition, the BVerfG has stipulated that the legislature has to make organisational and procedural provisions which counteract the risk of violation of personal rights. Thus, the judgment states, that e.g., prohibitions of disclosure and exploitation as well as obligations to clarify, inform and erase are regarded as essential procedural safeguards. Therefore, the basic ideas of purpose limitation/unlinkability, necessity, transparency and intervenability, as well as the security of the data processing can be deduced from the rulings of the BVerfG and, supported by the design of processes according to these ideas, protect the right to informational self-determination.

In the decision on secret access to information technology systems (BVerfG, ruling of 27 February 2008, 1 BvR 370/07 et al.), the BVerfG developed the basic right to integrity and confidentiality of information technology systems. In certain circumstances, information technology systems as a whole are also subject to an independent, person-related guarantee of confidentiality and integrity, and not just individual communication processes or stored data. However, according to the findings of the BVerfG, the scope of protection of the fundamental right is only admissible if:

- The data subjects are dependent on the use of the system for their personal development,
- It is possible that the system includes personal data of the data subject to such an extent and diversity that access to the system allows to gain insight into essential parts of a person's life or even to obtain a meaningful picture of the personality and,
- If the data subject uses the system as his or her own and accordingly assumes that he or she is self-determined in the use of the information technology system, either alone or together with other persons authorised to use it.

In such cases, the data subject may expect that his or her data generated, processed or stored by the information system to remain confidential and that the system cannot be accessed in such a way that its services, functions and contents can be used by third parties (unauthorised), which would imply that the technical obstacle for spying, monitoring or manipulating the system has been overcome. However, in cases where information technology systems are used by the data subjects as own systems but are operated by third parties, the fundamental right to ensure the integrity and confidentiality of information technology systems can be viewed as a direct constitutional guarantee of the protection goals of confidentiality and integrity. The indirect third-party impact of fundamental rights can also have an impact on the relationship between individuals and private organisations, for example in the case of cloud services for private individuals, which more and more fulfill a central back-up function for all digitised personal information or generate such information. In addition, mobile phones and / or smartphones can be regarded as information technology systems, which are to be protected considering the context of service use where these devices interact with the IT of public and private bodies. Insofar as the use of the own information technology system takes place via information technology systems, which are in the power of others, the protection of the user also extends to these systems.

6.2 Embedding the Protection Goals in the Federal Data Protection Act (BDSG)

6.2.1 Protection Goals as Review Standard

The starting point in German law is Section 9 (1) BDSG. The article states that:

> *"Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection."*

Section (9) (1) BDSG stipulates that the data protection requirements are to be ensured by implementation of technical and organisational measures. The legal consideration of whether "the effort involved in these measures is proportionate to the intended protection" must have already taken place and should have been decided during the planning phase, for ex-

ample in the context of an assessment to identify the required level of protection. The protection goals which, on the one hand, can bundle and structure the data protection requirements and, on the other hand, be achieved through technical implementation serve as a means of determination which measures may be appropriate and necessary and thus be adequate.

The controller is obliged to establish the appropriate technical and organisational measures in advance and to prove this accordingly. The BVerfG has stipulated in its census decision (BVerfG, ruling of 15 December 1983, 1 BvR 209/83) that the legislature has to take organisational and procedural precautions, which counteract the danger of the encroachment of personal rights. Section (9) (1) Federal Data Protection Act as well as clause 1 of the Annex to Section (9) Federal Data Protection Act are accordingly formulated: Only those who have previously shaped the internal organisation of authorities or enterprises in such a way that it meets the special requirements of data protection and only those who have taken the necessary and appropriate measures, can ensure that the regulations will be complied with for all subsequent events. Insofar as there is an obligation to specify the measures in advance (for example, in a safety concept that has to be prepared in advance), it must be possible to account for fulfillment of this obligation, in particular according to the requirements of the GDPR. The data protection directive 95/46/EC also states in recital 46 that appropriate technical and organisational measures are to be taken at the time of the planning of the processing system, in particular to ensure the security of the processing and to prevent any unlawful processing. The principle of prohibition of processing in Section (4)(1) Federal Data Protection Act obliges the controller to know in advance whether its planned data processing is permissible or not. At that time already, the controller must therefore be able to document that compliance with the provisions is also ensured by technical and organisational measures.

The data protection regulations can be assigned to the protection goals (so-called ‘mapping’), according to their importance and their objectives. This type of structuring enables the operationalisation of data protection requirements in an auditable and standardised form, as is has been a proven practice in the BSI IT-Grundschutz methodology since the mid-1990s. This way, the controller is also supported by providing evidence that the necessary measures to avoid legal infringements have actually been taken.

The following examples and the ‘mapping table are intended to clarify how the mapping can take place.

Data Minimisation

Section 3(a) of the Federal Data Protection Act (BDSG) specifies (deviating from the term Data Minimisation in the GDPR) the principle of data avoidance, which derives from the principle of necessity, the latter being the central statutory criterion for legitimacy of processing (e.g. Section 28 BDSG). The regulation of Section 3(a) clause 1 BDSG states clearly that the principle applies in particular to the selection and design of data processing systems.

Special requirements arise, for example, from the obligation to erase data if they are no longer necessary (Section 20 (2) (2) and Section 35 of the Federal Data Protection Act), or the anonymisation requirement in Section 30a (3) of the Federal Data Protection Act.

Availability

This protection goal is laid down in No. 7 of the Annex to Section 9 BDSG. The requirement to avoid the loss of the data also implies to maintain the usability of the data (and an ability to provide information about it) as a loss of this capability amounts - in its effects - to a loss of data with respect to the processing purpose.

Article 17 (1) first clause of the Data Protection Directive 95/46/EC also requires appropriate protection measures against the accidental or unlawful destruction or the accidental loss of personal data.

Integrity

From the requirements in No. 3 and No. 4 of the Annex to Section 9 BDSG to rule out unauthorised changes and erasure of data, the protection goal integrity at data level can be derived. The requirement of ensuring integrity at system level derives from the general principle of ensuring legally compliant data processing (Section 9 BDSG).

Article 17 (1) of Directive 95/46/EC also calls for the adoption of appropriate measures for protection against unauthorized modification of personal data. Furthermore, a "fundamental right to ensure the confidentiality and integrity of information technology systems" (see above) has been existing at least for the area of data processing in the public sector since the Federal Constitutional Court's decision of 27 February 2008 (BVerfG, 1 BvR 370/07).

Confidentiality

The obligation to maintain confidentiality results, in particular, from the protection obligation under No. 3 and No. 4 of the Annex to Section 9 BDSG, and from Article 16 and Article 17 (1) of the Data Protection Directive 95/46/EC and Section 5 BDSG (data secrecy).

Unlinkability

The obligation to process data only for the purpose for which it was collected is, in particular, derived from the legal basis for the individual processing which make the business or research purposes etc. a benchmark. For data processing on the basis of consent, Section 4a (1) clause 2 BDSG states that the controller has to indicate the intended purpose. Therefore, the purpose must be defined and the consent extends only to the processing for this purpose.

Article 6 (1) (b) and (c) of the Data Protection Directive 95/46/EC also imply that data processing must be based on an explicit and legitimate purpose.

In addition, the obligation to define the purposes is derived from the requirements for the creation of a procedure index or the reporting of automated procedures (Sections 4d (1), 4g (2) clause 1, 4 (e)) and from Section 28 (1) clause 2 BDSG.

The specific requirement for data separation is laid down in No. 8 of the Annex to Section 9 BDSG.

Transparency

The information provided in the Data Protection Directive 95/46/EC (Articles 10, 11, 12) as well as in the BDSG (Sections 4 (3), 4a (1) clause 2, 33, 34 BDSG), govern the rights of information, notification and access for the data subject. The controller must, in accordance with clause 1 of the Annex to Section 9 BDSG, create the necessary conditions for granting these rights both at organisational and, if necessary, at technical level.

Initially, Section 4 (1) BDSG creates the obligation for the *controller* to process personal data only on the basis of consent or a legal provision. Since the regulation is formulated as a principle of prohibition of processing subject to the possibility of permission, the controller must ultimately have examined whether a legal basis exists. All of this means that, as a general rule, the controller must know about all personal data being processed within his sphere of responsibility in order to be able to evaluate it. Specific requirements establishing internal transparency derive from Sections 4d (1), 4e and Sections 4g (2), 4e BDSG.

In addition, a public index of procedures, which forms a necessary part of a comprehensive overall documentation of a procedure, must be prepared. With the exception of technical and organisational measures, *anyone* can demand access to the index according to Section 38 (2) BDSG or Section 4g (2) clause 2 BDSG.

Intervenability

The data subject's rights to intervene are explicitly derived from the regulations on rectification, blocking, erasure and objection. They may also result from a weighting of interests within the framework of statutory criteria for permission. Again, the controllers must, in accordance with clause 1 of the Annex to Section 9 BDSG, provide the prerequisite for guaranteeing these rights both at organisational level and, where required, at technical level.

Table1: Allocation of the legal requirements of the BDSG to the protection goals

	Data minimisation	*Availability*	*Integrity*	*Confidentiality*	*Unlinkability*	*Transparency*	*Intervenability*
Sec. 3a	Sec. 3a						
Sec. 4	Sec. 4 (2) (a)				Sec. 4 (3) (2)	Sec. 4 (3)	Sec. 4 (1)
Secs. 4a, 4 b, 4c, 4d, 4 e, 4f, 4g					Sec 4a (1) clause 2 Sec. 4b (6) Sec. 4c (1) clause 2 Sec. 4e No.4	Sec. 4a (1) clause 2–4, (2) clause 2, Abs. 3 Sec. 4d (1) clause 1, Sec. 4d (5) Sec. 4e Sec. 4g (2)	Sec. 4c (1) clause 1 No. 1

	Data min-imisation	*Availability*	*Integrity*	*Confidenti-ality*	*Unlinkabil-ity*	*Transpar-ency*	*Intervena-bility*
Sec. 5				Sec. 5 clause 1, 2, 3			
Secs. 6, 6a, 6b, 6c	Sec. 6b (1), (3), (5)				Sec. 6 (3) Sec. 6b (1), Sec. 6b (3) clause 3, Sec. 6b (5)	Sec. 6 (1), (2) clauses 1-3 Sec. 6a (2) No. 2 Sec. 6b (2), (3), Sec. 6b (4) Sec. 6c (1), (3)	Sec. 6 (1), Sec. 6 (2) clause 1 Sec. 6a (1) clause 1, (2) No. 2
Sec. 9	Sec. 9 clause 1	Sec. 9 clause 1 No.7 Annex to Sec. 9	Sec. 9 clause 1 No. 3, No. 4, No. 5 Annex to Sec. 9	Sec. 9 clause 1 No. 3, No. 4 Annex to Sec. 9	Sec. 9 clause 1 No. 8 Annex to Sec. 9	Sec. 9 clause 1 No. 1-6 Annex to Sec. 9	Sec. 9 clause 1
Sec. 10					Sec. 10 (2) (No. 1)	Sec. 10 (2 and 3), (4) clause 3	
Sec. 11	Sec. 11 (2) clause 2 No. 10	Sec. 11 (2) clause 2 No. 3	Sec. 11 (2) clause 2 No. 3	Sec. 11 (2) clause 2 No. 3 Sec. 11 (2) clause 2 No. 10	Sec. 11 (2) clause 2 No. 2 Sec. 11 (2) clause 2 No. 10	Sec. 11 (2)	Sec. 11 (2) clause 2 No. 4
Secs. 28, 28 a	Sect. 28 (1) clause 1 No. 1, No. 2, (2), (3) clause 2, (6-9) Sec. 28a (1)	Sec. 28 (3a) clause 1	Sec. 28 (3a) clause 1		Sec. 28 (1) clause 1 nos. 1-2, (1) clause 2 ,(2), sect. 28 (3) clauses 1-5, clause 7, (5), (6-9) Sec. 28a (1), (2), Sec. 28a (2) clause 4	Sec. 28 (3) clause 4, clause 5, sec. 28a (3) Sec. 28a (2) clause 2, (3)	Sec. 28 (3a) clause 1, (4)
Sec. 29					Sec. 29 (1), (2), (4)	Sec. 29 (2) clause 2, clause 3, clause 4,	Sec. 29 (3), (4)

	Data min-imisation	*Availability*	*Integrity*	*Confidenti-ality*	*Unlinkabil-ity*	*Transpar-ency*	*Intervena-bility*
						(7) clause 1	
Sec. 30	Sec. 30 (1) Sec. 30a (3)						
Sec. 31					Sec. 31		
Secs.33–35	Sec. 35					Secs. 33–34	Secs. 33–35
Sec. 38						Sec. 38 (1) clause 5	
Sec. 39					Sec. 39		
Sec. 40	Sec. 40				Sec. 40		
Sec. 42a						Sec 42a	

6.2.2 Embedding the Applicability of the Protection Goals in Procedures Involving the Processing of Personal Data

Although the substantive legal requirements are mostly based on specific data processing operations, the controller's duty to prevent violations consequently demands the consideration of technical and organisational measures already during the design process so that they also can be incorporated in the actual data processing. The operationalisation of data protection requirements therefore requires focusing on the procedures involving the processing of personal data so that the protection goals which need to be achieved using those measures need to be applied to the procedure as well.

The Federal Data Protection Act (BDSG) contains a set of regulations which concern the procedure as such and lay down respective requirements (see Sections 4d (1), 4d (5), 6c (1), Section 10 (1), Section 28b No. 1, Section 29 (2) clause 3, Section 38 (5) clause 2, Section 43 (2) No. 2 BDSG). In some cases, statutory requirements are imposed on processing operations or procedures that do not (yet) contain any references to personal data or such reference cannot be excluded (Sections 11 (5) (b) No. 1, Section 34 (2–4), as well as, for example, Section 13 (1) clause 2 TMG). Procedures are explicitly referenced within the framework of reporting obligations and preliminary controls (Section 4e BDSG).

According to the latter, the law does not provide for a strict separation between specific data processing and procedural requirements, even in regard to the need for anchoring requirements.

6.3 Embedding the Protection Goals in the Data Protection Laws of the Länder

Initially, two categories have to be created. A number of national data protection laws therein foresee, like the BDSG does, specific assessments (Bremen, Hesse, Rhineland-Palatinate,

Saarland, Bavaria, Baden-Württemberg and Lower Saxony). For these Länder, the explanations on the BDSG above are valid (see 6.2).

Some data protection laws of the Länder state specific requirements as 'data protection goals.' (Schutzziele) and thus already reflect some protection goals ('Gewährleistungsziele'). The data protection laws of the new Länder as well as the data protection laws of Berlin, Hamburg and North-Rhine-Westphalia include the protection goals availability, integrity and confidentiality as well as transparency (not Hamburg), authenticity and traceability. Since January 2012, the Land of Schleswig-Holstein Data Protection Act includes the complete set of the above mentioned protection goals.

The respective regulations with regard to technical and organisational measures form the starting point. These regulations demand the guarantee of lawful data processing. In this regard it makes no essential difference whether the data protection goals are phrased in an exemplary way (Mecklenburg-Vorpommern ("in particular") or phrased conclusively. In any case, protection goals may arise not only directly from the regulations on data protection goals, but also from substantive provisions.

However, it is important to note that the legally defined specification of the data protection goal 'Transparency' differs from the identically named protection goal in the SDM. Whereas the former only includes the documentation of procedures, the latter also includes the authenticity and traceability of specific data processing operations as well as the rights of information, notification and disclosure. Thus, only the protection goals of 'Unlinkability', 'Intervenability' and 'Data Minimisation' have not yet been anchored in previously existing protection goals. However, in this regard reference may be made to the discussion above within the framework of the BDSG.

In the following mapping table, the Saxon Data Protection Act is examined as an example, as to how the existing regulations can be mapped to the SDM data protection goals.

Table 2: Mapping of the legal requirement in the Saxon Data Protection Act with the protections goals

Data minimisation	*Availability*	*Integrity*	*Confidentiality*	*Unlinkability*	*Transparency*	*Intervenability*
Sec. 9 (1) clause 2	Sec. 9 (2) No. 3	Sec. 9 (2) No. 2	Sec. 9 (2) No. 1		Secs. 9 (2) No. 4–6	
Sec. 20, 21 (2) clause 2 (Erasure/ Blocking when necessity is no longer given)				Sec. 4 (3) (purpose limitation when giving consent)	Sec. 4 (3) (informed declaration of consent)	Sec. 4 (1) No.2 (Consent/ Revocation)
Sec. 36 (2) (Pseudonym./ Anonym. in scientific research)				Sec 10 (1) clause 2 (Intended purpose in procedure log)	Sec. 5 (Rights of data subject)	Secs. (19–21) (Rectification, Erasure, Blocking)

Data minimisation	*Availability*	*Integrity*	*Confidentiality*	*Unlinkability*	*Transparency*	*Intervenability*
Sec. 33 (4) (Deadline for erasure of video recordings)				Sec. 12 (2, 5, 6) (Intended purpose on collection)	Secs. 3 ,10, 11 (4) No. 5, 31 (2) (Procedure log)	Sec. 32 (1) (Telemetry and Telecontrol)
Sec. 12 (Collection only in case of necessity)				Sec. 13 (Purpose limitation for storage etc.)	Sec. 12 (Data collection)	
Sec. 13 (Storage etc. only in case of necessity)				Secs. 14 (3), 16 (4) (Purpose limitation for transmission)	Secs. 18, 34 (3) (Provision of information)	
Secs. 14–17 (Transfer of data only in case of necessity)				Sec. 32 (1) (Purpose limitation for telemetry and telecontrol)	Sec. 27 (Monitoring)	
				Sec. 33 (Purpose limitation Video)	Sec. 32 (Telemetry and telecontrol)	
				Sec. 34 (Automated individual decision)	Sec. 33 (3) (Video surveillance)	

6.4 Embedding the Protection Goals in the European General Data Protection Regulation

The European General Data Protection Basic Regulation (GDPR) applies uniform rules for data protection legislation throughout Europe. The regulation, which entered into force on 25 May 2016, will, pursuant to Sec. 99 (2) GDPR be directly applicable in all EU Member States from 25 May 2018. National legislatures are given additional regulatory powers through numerous supplementary opening clauses (‘Öffnungsklauseln’). However, the GDPR fundamentally holds precedence over national law. The protection goals are most essentially laid down in the principles of the processing of personal data in Section 5 GDPR, which in turn include the protection order from Section 8 of the Charter of Fundamental Rights of the European Union.

Accordingly, the GDPR obliges the controller and processor to choose the appropriate technical and organisational measures to ensure the fundamental protection of the rights of the data subjects as well as measures against unauthorized access by third parties (in particular

Article 32 GDPR) and implement and check them within the framework of the technical design and data protection-friendly pre-settings pursuant to Article 25 GDPR (Article 32(I) (d). The controller is responsible for compliance with the principles of processing pursuant to Article 5 (1) and 24 GDPR and must be able to prove compliance with the principle. Furthermore, the GDPR demands for a data protection impact assessment for all types of processing with potentially high risk for the rights and freedoms of natural persons (Article 35 GDPR, DPIA (data protection impact assessment)) . It is based on a systematic description of the planned processing procedures and as a result calls for measures to overcome the expected risks. This includes guarantees, safety precautions and procedures which can be used to ensure, verify and evaluate the protection of personal data (Article 35 (7) and (11) GDPR). The SDM is intended to help organisations with the transition to the GDPR in a transparent, controlled and resource-conserving way. It is intended to contribute to implementing the principles set out in Article 5 for the processing of personal data and to achieve, with reasonable effort, the proof of implementation required by the GDPR (e.g. according to Article 5 (2) and Article 24 (1)).

The SDM can also be an appropriate resource in respect of transferring personal data to third countries or to international organisations. By means of the SDM, it is possible to derive technical and organisational measures to provide for suitable guarantees pursuant to Article 46 GDPR or for binding internal rules for the protection of personal data (Binding Corporate Rules - BCR) pursuant to Article 47 GDPR. The SDM, for example, supports the selection of appropriate and proportionate measures for procedures, in particular with regard to documentation and logging, which have been requested by data protection supervisory authorities in several countries as the state of the art for years.

The protection goals Integrity, Availability, Confidentiality, Transparency and Data Minimisation can be found conceptually in the text of the regulation, while also referring to IT security requirements. The protection goals Unlinkability and Intervenability have been adopted as data protection goals in numerous individual articles of the GDPR, *inter alia* via the principle of purpose limitation, erasure and data portability.

The following explanations and tables provide an overview of the implementation of protection goals in the articles and recitals of the GDPR.

Availability

The principle of *availability* is explicitly included in Article 32 (1) (b) and (c) in the context of security of data processing. It is also anchored in Article 5 (1) (e) GDPR as a prerequisite for the identification of the data subject. It ensures the availability of the data for the respective purpose as long as this purpose remains valid. The principle applies to the obligations to provide information and access to the data subject (Articles 13 and 15 GDPR). The protection goal availability is also a basic prerequisite for the right to data portability (Article 20 GDPR).

Integrity

The protection goal *integrity* is mentioned in Article 5 (1) (f) GDPR as a principle for the processing of data and in Article 32 (1) (b) GDPR as a prerequisite for the security of data processing. It shall ensure protection against unauthorized modifications and deletions.

Confidentiality

The obligation to maintain *confidentiality* results, in particular, from Article 5 (1) (f) GDPR, from Article 32 (1) (b) GDPR and Article 38 (5) GDPR (secrecy obligation of the data protection officer) and Article 28 (3) (b) GDPR (secrecy obligation of the data processor) respectively. It ensures the protection against unauthorized and unlawful processing. A violation of confidentiality in general constitutes a data processing without a legal basis.

Unlinkability

The obligation to process data only for the purposes for which they were collected is to be found, in particular, in the individual legal basis for processing (Art 6 GDPR) that make the business purposes, the research purposes, etc. a yardstick. It is included in the General Data Protection Regulation through the principle of purpose limitation in Article 5 (1) (b). In the case of data processing on the basis of consent, it is derived from Article 7 (4) GDPR that consent can be invalid if the data is not necessary to fulfill the purpose.

A typical measure for *unlinkability* is, for example, pseudonymisation as mentioned in Article 40 (2) (d) GDPR.

Transparency

The principle of *transparency* is laid down in Article 5 (1) (a) GDPR. It is reflected as a fundamental principle of data protection law in numerous regulations of the GDPR. Especially the obligations to information and access take this principle into account.

Intervenability

The data subject's rights to *intervene* are explicitly derived from the provisions on rectification, blocking, erasure, and the right of objection (Articles 16-17 GDPR). They may also result from a weighting of interests within the framework of statutory criteria for lawful processing. Once again, the controller must, pursuant to Article 5 (1) (d) GDPR provide the prerequisite for guaranteeing such rights, both at organisational and, where required, at technical level.

Table3: Allocation of the articles of the GDPR to the Protection Goals

Data minimization	*Availability*	*Integrity*	*Confidentiality*	*Unlinkability*	*Transparency*	*Intervenability*
5 (1) (c), 5 (1) (e), 25, 32	5 (1) (e), 13, 15, 20, 25, 32	5 (1) (f), 25, 32, 33	5 (1) (f), 25, 28 (3) (b), 29, 32	5 (1) (c), 5 (1) (e), 17, 22, 25, 40 (2) (d)	5 (1) (a), 13, 14, 15, 19, 25, 30, 32, 33, 40, 42	5 (1) (d),5 (1) (f), 13 (2) (c), 14 (2) (d), 15 (1) (e), 16, 17, 18, 20, 21, 25, 32

Table 4: Allocation of recitals in the GDPR to the Protection Goals.

Data Minimisation	*Availability*	*Integrity*	*Confidentiality*	*Unlinkability*	*Transparency*	*Intervenability*
28, 29, 30, 39, 78, 156	49, 78, 83	39, 49, 78, 83	39, 49, 78, 83	31, 32, 33, 39, 50, 53, 71, 78	32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100	39, 59, 65, 66, 67, 68, 69, 70, 78

7 The generic measures for the implementation of the Protection Goals

For each of the SDM's components (data, systems, and processes), reference measures are named and described in the Annex for each of the protection goals. For each of the measures, the effects of implementation for other protection goals which are not directly affected by the respective measure shall also be considered. This way, specific measures can contribute individually to the achievement of several protection goals.

This Section lists generic data protection measures that have been tried and tested in data protection investigations and audits 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 specific reference measures can be found in the catalogue of measures (Annex).

7.1 Data Minimisation

The protection goal *data minimization* can be achieved by:

- Reduction of collected attributes of the data subject,
- Reduction of processing options in processing operations,
- Reduction of possibilities to gain knowledge of existing data,
- Preference for automated processing operations (not decision-making processes), which make the use of processed data unnecessary and limit the possibility of interference, compared to dialogue controlled processes,
- Implementation of automatic blocking and erasure routines; procedures for pseudonymisation and anonymisation,
- Rules to control processes for the change of procedures.

7.2 Availability

Typical measures to guarantee *availability* are:

- Preparation of data backups, process states, configurations, data structures, transaction histories etc., according to a tested concept,
- Protection against external influences (malware, sabotage, force majeure),
- Documentation of data syntax,
- Redundancy of hard- and software as well as infrastructure,
- Implementation of repair strategies and alternative processes,
- Rules of substitution for absent employees.

7.3 Integrity

Typical measures to guarantee *integrity* or to assess a breach of integrity are:

- Restriction of writing and modification permissions,
- Use of checksums, electronic seals and signatures in data processing in accordance with a cryptographic concept,
- Documented assignment of rights and roles,
- Processes for maintaining the timeliness of data,
- Specification of the nominal process behaviour and regular testing for the determination and documentation of functionality, of risks as well as safety gaps and the side effects of processes,
- Specification of the nominal behaviour of workflow or processes and regular testing of the detectability respective determination of the current state of processes.

7.4 Confidentiality

Typical measures to guarantee c*onfidentiality* are:

- Definition of a rights and role concept according to the principle of necessity on the basis of identity management by the controller,
- Implementation of a secure authentication process,
- Limitation of authorized 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,
- Specification and control of the use of approved resources, in particular communication channels,
- Specified environments (buildings, rooms) equipped for the procedure,
- Specification and control of organisational procedures, internal regulations and contractual obligations (obligation to data secrecy, confidentiality agreements, etc.),
- Encryption of stored or transferred data as well as establishing processes for the management and protection of the cryptographic information (cryptographic concept),
- Protection against external influences (espionage, hacking).

7.5 Unlinkability

Typical measures to guarantee *unlinkability* are:

- Restriction of processing, utilization and transfer rights,
- In terms of programming, omitting or closing of interfaces in procedures and components of procedures,
- Regulative provisions to prohibit backdoors as well as establishing quality assurance revisions for compliance in software development,

- Separation in organisational / departmental boundaries,
- Separation by means of role concepts with differentiated access rights on the basis of an identity management by the responsible authority and a secure authentication method,
- Approval of user-controlled identity management by the data processor,
- Using purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymous data,
- Regulated procedures for purpose amendments.

7.6 Transparency

Typical measures to guarantee *transparency* are:

- Documentation of procedures, in particular including the business processes, data stocks, data flows and the IT systems used, operating procedures, description of procedure, interaction with other procedures,
- Documentation of testing, approval and, where appropriate, prior checking of new or modified procedures,
- Documentation of the contracts with internal employees; contracts with external service providers and third parties, from which data are collected or transferred to; business distribution plans, internal responsibility assignments,
- Documentation of consents and objections,
- Logging of access and modifications,
- Verification of data sources (authenticity),
- Version control,
- Documentation of the processing procedures by means of protocols on the basis of a logging and evaluation concept,
- Consideration of the data subject's rights in the logging and evaluation concept.

7.7 Intervenability

Typical measures to guarantee *intervenability* are:

- Differentiated options for consent, withdrawal and objection,
- Creating necessary data fields, e.g. for blocking indicators, notifications, consents, objections, right of reply,
- Documented handling of malfunctions, problem-solving methods and changes to the procedure as well as to the protection measures of IT security and data protection,
- Disabling options for individual functionalities without affecting the whole system,
- Implementation of standardised query and dialogue interfaces for the persons concerned to assert and/or enforce claims,
- Traceability of the activities of the controller for granting the data subject's rights,
- Establishing a Single Point of Contact (SPoC) for data subjects,

- Operational possibilities to compile, consistently correct, block and erase all data stored with regard to any one person.

8 The Procedure Components

The term ‘procedure’ is used to describe complete data processing operations. Data processing means, in particular, any collection, storage, modification, transmission, blocking, erasure, use, anonymisation, pseudonymisation and encryption of personal data. A procedure describes a formalised, repeatable sequence of the above-mentioned steps of data processing to realise a specialist task or a business process. Hereby, it does not matter whether these are executed manually, or by means of information technology. A procedure is always characterised by its purpose and is thereby differentiated from other procedures.

The following three components are to be distinguished when setting up a procedure with reference to persons, because on the level of measures, their contributions to the implementation of the protection goals differ:

- Personal data,
- Technical systems involved (hardware, software and infrastructure), as well as
- Processes with regard to organisation and human resources involved when processing of data with the systems.

In terms of methodology, the initial focus is on personal data, whose level of protection has to be determined or specified by the controller. The systems and processes inherit this protection level. On the basis of the reference catalogue of data protection measures, it can be checked whether the measures taken or planned for a procedure are appropriate and match with the required protection level.

For these three core components, the following properties, *inter alia*, play an important role:

It is necessary to look at the properties of *data formats* that are used to collect and process data. Data formats can have an impact on the quality of the implementation of the protection goals, for example in those cases where it is not yet resolved conclusively which content files contain in specific formats (e. g. old, supposedly erased data stock of a text file that does not show when printed; metadata concerning, for example, the camera model, location and time of graphics files), or when it is a matter of lossy files (e.g. graphics, video or audio files in which relevant information are lost due to compression).

For the systems involved, it is necessary to consider those *interfaces* which have a connection to other systems not being within the system limit defined by the purpose of the processing. The registration of existing interfaces as well as the documentation of their properties is of crucial importance for the control and verification of data flows.

For each process, *responsibilities* have to be clarified, which are typically specified and assigned as roles in a comprehensive role concept. The responsibility of a process owner covers all core and relief processes in the field of technology and organisational assignments or in the field of content-related data processing or, consistently covers all process levels of one

procedure in the sense of an overall process responsibility. This responsibility can be delegated to several roles. It is of crucial importance to determine which of the participating organisational instances has to actively ensure the legitimacy of a data processing procedure.

Especially for the consideration of process and procedure responsibilities, it is important to take into account that procedure components can be classified either as parts of an organisation-wide process, or as independent sub-processes. In both cases, the assignment of the responsibilities must be clear.

9 The Protection Levels

Any processing of personal data by an organisation constitutes an interference with the right to informational self-determination. This also applies to such processing that is permissible from a data protection point of view, i.e., on the basis of a legal ground or a valid and informed consent. Therefore, an organisation must prove that it limits this interference to the degree absolutely necessary, thus minimizing the level of interference (see, for example, Article 5 (2) and Article 24 (1) GDPR). It can provide verification by outlining how the protection goals are realised.

In this model, the term 'organisation' refers to public bodies, private companies and to other institutions, such as scientific institutes. The term 'organisation' covers both the responsible body and the contractor in the context of commissioned data processing in the sense of the German data protection law, or the controller and the processor in the sense of the General Data Protection Regulation (GDPR).

When determining the level of protection, the SDM takes the perspective of the data subject and her/his exercise of fundamental rights, and therefore differs from the point of view of IT-Grundschutz.

IT-Grundschutz is primarily concerned with information security standards and focusses on the primary objective of protecting the data-processing organisation. For the specification of the level of protection according to the SDM, the *level of interference* which the data processing by the organisation represents to the data subject is decisive.

9.1 Level of Interference

To be able to assess the required level of protection of information security, it is methodically customary to measure the amount of damage and occurrence probability, and to evaluate the resulting risk thereof. However, the protection (of fundamental rights) of individuals is not the focus of this method. In order to be able to evaluate the significance of the risks to the right to informational self-determination and which individual level of protection result from a procedure, the level of interference on the fundamental rights must be evaluated by means of a procedure. A measure for the level of interference is, *inter alia*, the purpose of the data processing that is determined by the corresponding legal basis, the level of protection, the duration of storage, the type and the number of possible recipients of the processed data. Thus, the application of the SDM can lead to the conclusion that the level of protection for a business process does not correspond to the level of protection required to ensure the fundamental rights of the data subjects.

9.2 The Special Role of the Protection Goal Confidentiality

The protection goal *confidentiality* plays a special role in determining the level of protection. The confidentiality of personal data must be ensured by appropriate measures, even if the

level of interference with the right of informational self-determination is low. At this point, SDM and BSI-Grundschutz methodology have a quite large overlap. An organisation's requirements for the security of its own IT infrastructure are largely in line with the requirements of the data subject to ensure the confidentiality of her/his data. Therefore, the selection of measures for the protection of personal data is broadly equal to the selection of measures intended to ensure that requirements of baseline protection (Grundschutz) for appropriate information security is realised.

9.3 Granularity of Protection Levels

The SDM assumes that the level of protection is classifiable with regard to the interference arising from the processing of data. Based on the BSI's IT-Grundschutz methodology, the SDM differentiates the three protection categories 'normal', 'high' and 'very high' for procedures of personal data processing.

Level of protection category 'normal'

Since *any* processing of personal data is an interference with the fundamental rights of the data subject, the level of protection can - according to the SDM - never be below 'normal'. For this reason, it must be assumed that each procedure involving the processing of personal data requires at least a *normal* level of protection. A lower level of protection may consequently only exist when the processing of data does not involve personal data.

Level of protection category 'high'

The following examples of processing scenarios imply a level of interferences which can result in a *higher* level of protection:

- Processing of non-modifiable personal data, which, for a lifetime, can serve as an anchor for profiling, i.e., can be assigned to an identifiable natural person (e.g., biometric data, genetic data),
- Dissemination of unambiguously identifying, highly linkable data (e.g., valid health insurance number valid throughout the life time of a data subject, tax ID),
- Legally or otherwise to-be-justified lack of transparency for the data subjects with regard to procedures (e.g., State Protection, estimated values in scoring),
- Processing of data in procedures with potentially serious financial consequences for the data subject,
- Processing of data in procedures with potential consequences for the status / reputation of the data subject,
- Processing of data in a procedure with potential consequences for the physical integrity of the data subject,
- Processing of data which realistically can have impact on the exercise of fundamental rights of a large number of data subjects (e.g., in the case of increasing and area-wide public video surveillance),
- Risk of discrimination, stigmatisation (e.g., by means of algorithms, non-transparent accomplishment of decisions concerning a data subject),
- Intervention in particularly protected areas of life of a data subject.

Furthermore, a high level of protection for procedures involving the processing of personal data exists when the data subject is dependent on the decisions or services of an organisation (e.g., in benefit administration or in the medical field) and when an organisation:

- Is processing data with an extensive level of interference, which may lead to substantial consequences for the data subject,
- Processes data which are legally labelled as being particularly worthy of protection,
- Fails to provide real, demonstrably effective means of intervention and self-protection for the persons concerned.

A high level of protection is also required where it is not possible to settle conflicts under realistically manageable conditions before the Courts (e.g., providers of telecommunication services without local branches). The GDPR tackles to solve this problem by introducing the *lex loci solutionis (Marktortprinzip).*

In some cases, the legislator has explicitly laid down the level of protection in the legislative texts. For example, the BDSG stipulates in Sections 13 (2) and 28 (6–9) and 29 (5) specific regulations for 'special categories of personal data'. These provisions can be found in partially identical form in other data protection acts, respectively in the GDPR (e.g., Article 35 (3)). When these particular types of personal data are processed, there is in general no leeway for consideration and a 'high level of protection' must be applied.[1]

Level of protection category 'very high'

A *very high* level of protection is required for processing in which a data subject is directly and with vital significance dependent on the decisions or services of an organisation. Additional risks arise where the effects of a processing cannot come to the attention of the data subject.

9.4 Collision Between the Required Level of Protection for Information Security and for Fundamental Rights

IT-Grundschutz pursuant to the BSI also uses an assessment to identify the required level of protection. Because of the different objectives of IT-Grundschutz and SDM, it cannot be ruled out that the ascertainment of the required level of protection according to Grundschutz and according to SDM may produce different results for the same processing. However, in IT-Grundschutz, personal data are also considered requiring a particularly high level of protection. Since information security must be guided by fundamental rights oriented considerations too, a properly performed ascertainment of the protection level based on IT-Grundschutz should come to the same conclusions as an ascertainment of the protection level in line with SDM.

[1] In general, it would be desirable to work towards the specific determination of the level of protection of data in legislative proposals.

In exceptional cases of deviating assessments, however, the level for protection must be given priority in accordance with the data protection principles of SDM. The following example shows that such deviating results cannot be ruled out: The logging of employee behaviour, or the monitoring of external users in order to prevent information security attacks, can be assessed differently from the viewpoint of data protection as compared to information security. With regard to the determination of the protection level, such cases must be specifically treated, documented and, if necessary, justified.

9.5 Cumulative Effects

The required level of protection must be considered for each of the components data, systems and processes, which have already been described under Section 8. In practice, it has been proven methodically to start with determining the required level of protection of the data with regard to the processing purpose. This level is inherited by the respective systems and processes as further components of a processing procedure. Thereby, two types of cumulative effects have to be considered:

- Data with a normal level of protection may require a high level of protection, if they are processed in large quantities (‘Accumulation of a great number of data’).
- Data with a normal level of protection may require a high level of protection, if they are processed by persons who have different roles with varying rights for different purposes (‘Accumulation of a great number of rights’).

9.6 Risk Analysis

In addition to the consideration of the interference with fundamental rights, a risk analysis is necessary, which is intended to evaluate the likelihood that the organisation will not comply with data protection rules, despite all the measures taken to protect fundamental rights. On the basis of this risk analysis, it is possible that additional protective measures become necessary, which supplement the measures resulting from the level of interference.

Such a *data protection risk analysis* can also concern those aspects of information security, which serve to ward off – also in the interest of protecting the data subjects – unauthorized access as well as access that might imperil the integrity of personal data. The data protection risk analysis also looks at those organisations that are authorised to process data. In particular, the following four aspects shall be recorded and evaluated:

1. The strength of an organisation's motivation to *modify* the *purpose* of the data usage in an unauthorised way has to be assessed.
2. It is necessary to evaluate the *operational possibilities* which exist for an organisation for an unauthorised change of the data processing purpose, provided that the motivation for such a change of purpose is given.
3. The effects of the transfer of personal data *to third countries* must be taken into account. Irrespective of the determined level of protection for the data in the national

context, it must be examined which additional protective measures would be necessary for such a transfer and eventually, for the processing, in third countries.

4. The extent *of adopted measures for information security* must be evaluated, including the processes for resolving conflicts between safeguarding the information security of the business processes and the operational safeguarding of data protection law for the data subjects.

9.7 General Approach for High Level Protection

To achieve a high level of protection often results in the need for implementing additional measures in order to meet the protection goals. Appropriate measures are specified in the respective module blocks of the reference catalogue of data protection measures. At the same time, the measures appropriate for the normal protection level must be continued and their execution adapted to the higher level of protection.

On the one hand, this can be done by increasing the impact of a measure, provided that it provides the possibility for such a scaling. An example would be the increase of the length of cryptographic keys used. On the other hand, the adaptation can be carried out by ensuring a greater reliability in the specified execution of the measure. For this, it is necessary to determine possibly disruptive influences - technical errors, misconduct by users, force majeure and external influence – and then to increase the robustness of the measure by additional precautions which may often be of an organisational nature.

This iterative process is to be continued until threats for the protection goals are excluded with sufficient reliability with regard to the respective required level of protection. Verification of this effect must be documented in the risk analysis.

10 Auditing and Consulting on the Basis of the Standard Data Protection Model

The following Section is intended to provide information for the use of the Standard Data Protection Model in investigation and consulting activities of the data protection authorities.

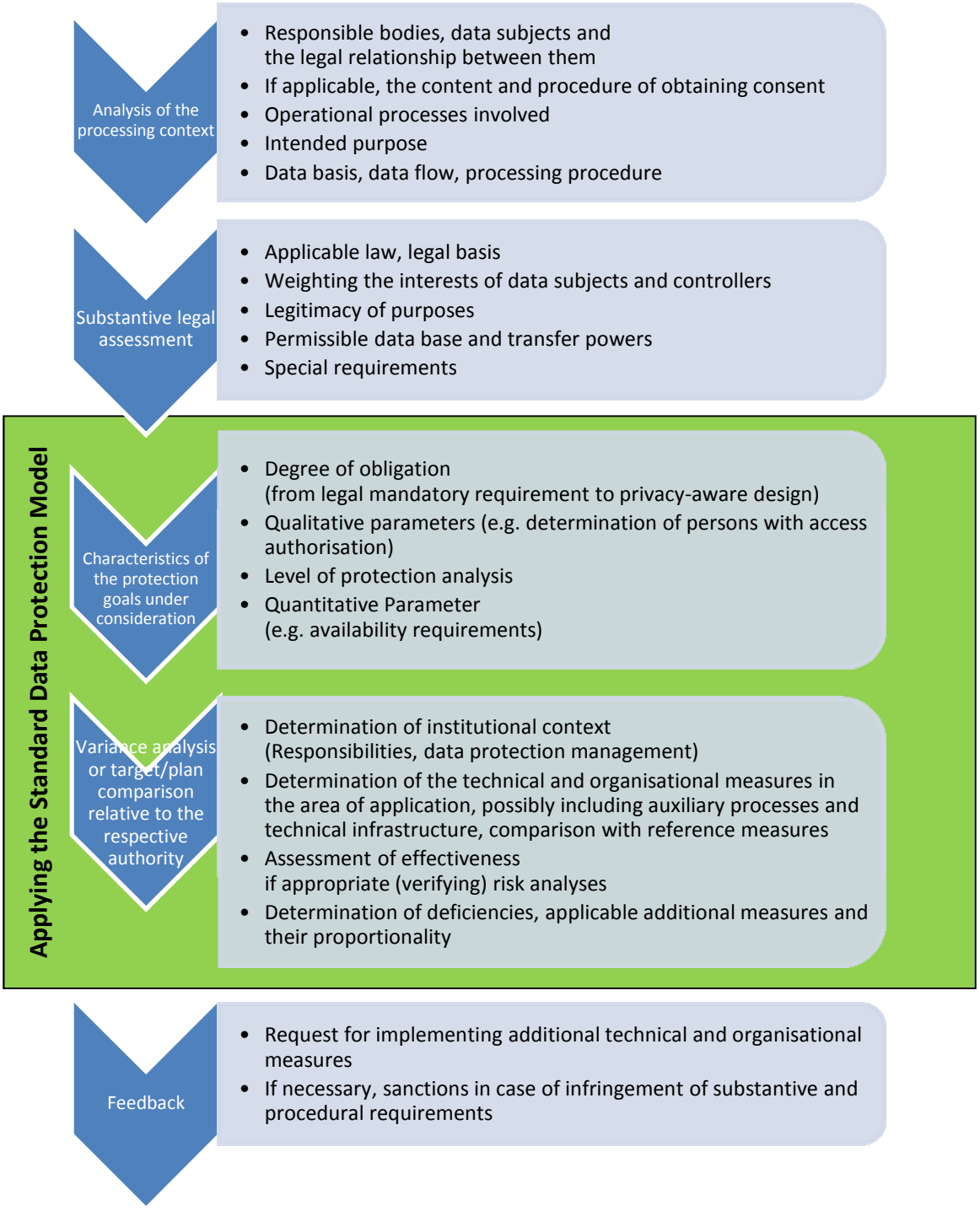

Figure 1. Application of the Standard Data Protection Model within the framework of investigation and consulting activities

A beneficial application of the model preconditions that the objective pursued by the process has been clarified in advance. In the rarest of cases, a data protection authority comprehensively examines the data processing of a responsible body. Usually, requests for consultation also focus only on specific aspects of a procedure, or the use of a specific technology. The evaluation or consulting object matters are limited both in terms of factual circumstances to be addressed and the requirements to be considered. Subsequently, a selection of the statutory requirements, which are embodied in the protection goals, must be made and which are then to be considered in the procedure. This is assumed in the following.

An overview of a purposeful use of the SDM is given in figure 1. In consultations, there may be the need to use a cyclic approach and to go through individual phases several times to the extent of the processing context getting adapted to the requirements of data protection.

There are two prerequisites for the application of the SDM: firstly, clarity about the factual circumstances within which the data processing to be considered should take place, and secondly, a substantive assessment of this processing.

In the light of these requirements and under the objective of the consulting or evaluation process, it is possible to determine in which way the protection goals are to be applied and viewed in the procedure, as well as to assess the required level of protection in the individual dimensions of the model. When applying the model, a set of technical and organisational reference measures can be derived thereof, which can be used to compare the intended measures or those identified in the test. This comparison also includes determining to what extent deficiencies in the application of the reference measures are offset by alternative measures. Upon conclusion, an evaluation of the remaining risks for the informational self-determination of the persons concerned is made and eventual ways of reducing these risks to an acceptable level with proportionate additional measures.

This evaluation resulting from the application of the model may subsequently serve as the basis for the recommendation or the request to remedy technical or organisational deficiencies, or to refrain from processing, provided that a sufficient risk reduction cannot be achieved by means of proportionate measures.

The above-mentioned steps are considered in more detail below.

10.1 Preparation

The substantive evaluation as well as the application of the SDM to evaluate the technical or organisational measures undertaken or planned, are both based on the determination of the factual circumstances for the processing. This includes, in particular, the following questions:

- Who is responsible?
- Is the processing carried out to fulfil the task of a public authority?
- Does a legal transaction or a similar legal obligation exist between the controller and the data subject?

- Does the consent of the data subjects form the legal basis of the processing and, if so, what content does the consent have and how is it obtained?
- If several controllers or processors are involved in the processing, how are the legal relationships between them regulated?
- For which purposes is the processing done and which business processes of the controller(s) are supported by the processing?
- Which data are collected, processed and used in which steps, via which systems and networks, and are utilized under the control of which persons?
- What auxiliary processes are used to support the processing?
- What kind of technical infrastructure is used?

Comprehensiveness and the degree of detail in the determination of the factual circumstances will vary from one operation to another, as well as the degree of the approach formalisation from informal questioning to the use of standardised questionnaires will. However, a structured summary of the results is as customary as it is indispensable for the further steps.

The substantive evaluation after the determination of the factual circumstances is focused on whether the examined or planned processing is generally permissible. It also provides answers to the following questions which are relevant to the subsequent application of the SDM:

- Which law is applicable to the processing?
- What purposes can be pursued legitimately with the processing, and what changes of purpose over the course of the processing are permissible?
- Which data are relevant or necessary for the fulfilment of the permitted purposes?
- Which legal basis for the transfer of data does exist between the involved entities and from those to third parties?
- What are the restrictions on the disclosure of processed data to persons beyond the involved entities?
- What special requirements must technical and organisational measures fulfil?

Such special requirements may arise, on the one hand, due to specific statutory regulations. On the other hand, situations may arise in which only the fulfilment of these requirements within the context of a weighing of interests can outweigh the data subject's interests in a preclusion of processing.

10.2 Characteristics of the Protection Goals

The extent to which the protection goals are to be formulated for the data processing in question depends primarily on the applicable law for the data processing - the control catalogues of the BDSG and of a number of State Data Protection laws (LDSG) or the protection goals catalogues of the other LDSGs - and whether the application of the SDM is carried out within the framework of an investigation, or in the context of a consultation in which, in ad-

dition to compliance with the legal minimum requirements, a data protection-friendly design is also aimed at.

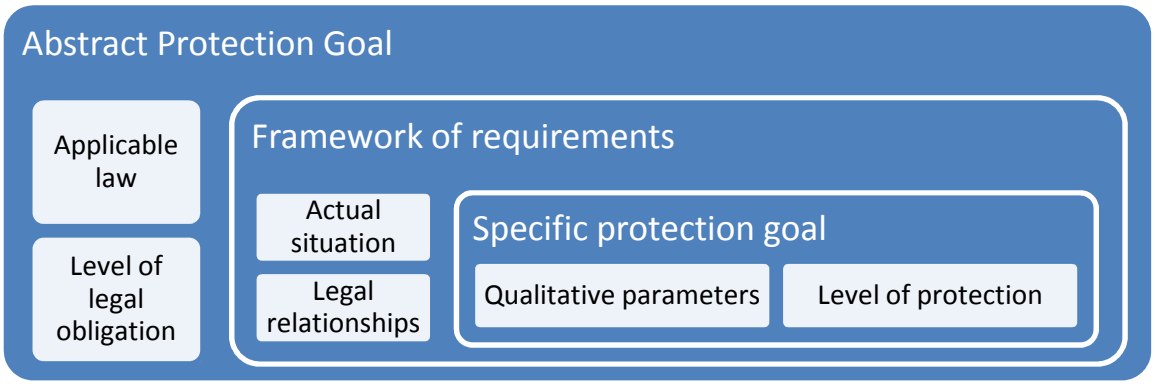

Figure 1: Characteristics of the Protection Goals

Based on the chosen characteristics, the protection goals to be considered must be defined further qualitatively and, where possible, technology-neutral:

1. *For whom within which processes must the availability of which data be ensured?* The influence of the possibility of the proper utilisation of the data in the interest of the data subjects is the benchmark for the concretisation of the protection goal Availability. The protection goal only applies to such data and those business processes where a loss of availability is contrary to the interests of the data subjects.
2. *What data should be kept intact, which should be kept up-to-date?* Again, the interest of the data subjects is the benchmark. In terms of ensuring timeliness, it is important to take into account the fact that topicality is generally only to be obtained with additional collection and processing procedures, which may possibly be contrary to the interests of the data subjects.
   The extent to which the integrity of the processes and systems must be ensured is derived from the concretisation of the other protection goals.
3. *To whom must the disclosure of which data be denied?* The extent of authorised access must be derived initially technology-neutral from the respective business processes. This defines the framework within which the measures for the protection of confidentiality against unauthorized personnel of the controller(s) should be established. The framework for the disclosure of data to third parties is given by the transfer permission identified in the substantive analysis.
4. *For whom and in which form is data processing to be kept transparent?* The requirements for the process documentation according to Section 4e BDSG, for the internal documentation of the processing procedures and their evaluability, as well as for the revision capability of the processing have to be laid down.
5. *Which rights of data subjects are to be granted to which extent?* Which data subjects must be notified of the automated processing? What data are to be included under which conditions for disclosure? Under which conditions must data be erased or blocked?

6. *What changes to the purposes are permissible? What purposes of auxiliary processes are legitimately derived from core processes? Only* statements for those purposes actually pursued or intended to pursue by the responsible authorities are needed. 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.
7. *The knowledge and the exercise of which disposition power by which persons and authorities over which data of the data subjects must be minimised?* Once again, the starting point for the evaluation is the interest of the data subjects to limit the burden to the extent absolutely necessary, even for a processing with permissible purposes.

Once the protection goals have been defined in terms of quality, a level of protection analysis must be carried out or, respectively, the level of protection analysis of the controller(s) or bodies must be understood. The procedures are set forth in chapter 9. Their result must be taken into account for further considerations in three ways.

Firstly, the protection goals can be refined further in a quantitative way. Examples of such refinements are answers to the following questions: For which period and to which degree is the loss of the availability of the data for the data subjects tolerable? With what delay shall the timeliness of the data be guaranteed? How precise in terms of time must it be possible to retrace the processing subsequently? What is the timeframe in which the controller must be able to ensure the respective rights of the data subject?

Secondly, the result of the protection level analysis forms the basis for the weighting between the protection of the data subject's interests and the effort required by the controller(s). For typical processing contexts, the result of such a weighting is outlined in chapter 7 by presenting reference measures which have to be implemented usually.

Thirdly, the result of protection level analysis is included in the assessment of the residual risks after implementing the measures, which can be taken in proportionate relation to the purpose of the processing. These risks regularly depend on the interest of third parties, or parties involved in the process, to violate protection goals, be it for gaining unauthorized access to the data of the data subjects in order to use, store, transmit or otherwise process it for illegitimate purposes, beyond the required extent, or in a non-transparent manner.

10.3 Target-Actual Comparison

The core element of the Standard Data Protection Model application is the comparison of the reference measures, which can be derived from the examined and, as stated above, specified protection goals, with the measures planned by the controller or, respectively, those determined in the investigation. Deviations are to be weighted and evaluated with focus on the extent to which they jeopardize the achievement of the protection goals. In an investigation process, the analysis carried out up to this point allows to draw conclusions from a failure of fulfilling the protection goals to (possibly sanctionable) data protection deficiencies.

In the practice of investigation and evaluation, it can often be determined with little effort that requirements are not fulfilled because the correspondingly assigned measures are obviously missing. The situation is more complex if the body to be examined has chosen other than the reference protection measures. Although these can be judged to be generally appropriate, it must be examined separately whether they actually corresponded to the specified level of protection. At this point, the SDM helps to focus the discussion on the verification that (or to which extent) the protective measure taken is functionally equivalent to the reference measure

11 The Operating Concept for the Standard Data Protection Model

11.1 Introduction

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

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

11.2 Contractor, Project Management, User

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

The development and maintenance of the SDM is carried out by the working group *Technology* of the DSK (AK Technik). The AK Technik is responsible for the project management.

The SDM can be used by the sixteen national data protection officers, the Bavarian State Office for Data Protection Supervision, as well as the Federal Data Protection Commissioners within the framework of their legal consulting, investigation and sanctioning activities (*user group 1*) as well as by the controllers (especially by the official and company data protection officers) for the planning and operation of procedures for the processing of personal data (*user group 2).*

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

- Creation and maintenance of the SDM, including the reference catalogue of data protection measures;
- Provision of the SDM and the reference catalogue of data protection measures;
- Processing of change requests (CRs) to the SDM, which can be introduced by both user groups, and for which the DSK must decide on their acceptance;
- Ensuring the quality of the work results;
- Version control for the SDM;
- Project management, including:
    - Provision of a Single Point of Contact (Service desk),
    - Operation of CR tracking,

    - Moderating discussions,
    - Administration of necessary means (website, project platform);
- Public relations.

12 Catalogue of Reference Measures

The catalogue of reference measures will become an integral part of the SDM but will be revised in shorter cycles than the SDM itself – depending on the technical development – and according to the specifications of the operating model (see Chapter 11).

13 Keyword Index