European Cloud Service
Data Protection Certification

AUDITOR Concept of Protection Categories

- Draft version 0.2 -

As of 28.03.2019

Related AUDITOR publications:

- object of certification
- criteria catalogue
- DIN SPEC 27557

Online available: www.auditor-cert.eu

Recommended Citation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR Concept of Protection Categories – Draft version 0.2. Karlsruhe, Germany: KIT. Online available: www.auditor-cert.eu

Contribution to the research project "European Cloud Service Data Protection Certification (AUDITOR)", which is funded by the German Federal Ministry for Economic Affairs and Energy (FKZ 01MT17003A), based on a decision made by the German Parliament.

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Authors

Alexander Roßnagel[a], Ali Sunyaev[b], Sebastian Lins[b], Natalie Maier[a], Heiner Teigeler[b]

[a] Project group Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG) at Kassel University

[b] Critical Information Infrastructures (cii) research group at the Institute of Applied Informatics and Formal Descriptive Methods (AIFB) at Karlsruhe Institute of Technology

Disclaimer

Please note that the AUDITOR consortium publishes all project-related findings initially in German and then translates them into English. Consequently, this document might contain linguistic or wording errors, for example, concerning the form for the expression of provisions (i.e., using shall, should, must, may and can). The AUDITOR consortium tries to continuously improve all documents to achieve a high level of maturity. If you identified any errors or have any concerns, please do not hesitate to contact the AUDITOR consortium (info@auditor-cert.eu).

Table of contents

List of abbreviations

Art.	article
BDSG	Federal Data Protection Act
e.g.	for example
GDPR	EU General Data Protection Regulation (valid as of 25.05.18)
Lit.	litera
No.	number
Para.	paragraph
TCDP	Trusted Cloud Data Protection Profile

Note on gender-neutral wording:

For reasons of easier readability, gender-specific differentiation is dispensed with. Those types of terms apply to all genders in the sense of equal treatment.

Note on AUDITOR as TCDP successor:

Certification according to the former German Federal Data Protection Act (BDSG) was examined in the pilot project “Data Protection Certification for Cloud Services” by the Trusted Cloud Data Protection Profile (TCDP), finalised in September 2016. TCDP represents an audit standard for the Data Protection Certification for Cloud Services according to the former Federal Data Protection Act and distinguishes three protection categories, which are described in the Concept of Protection Categories. The research project AUDITOR developed a standard for the data protection certification of cloud services according to the General Data Protection Regulation (GDPR) as the successor to TCDP. The AUDITOR criteria catalogue distinguishes three protection categories for technical and organisational measures for data protection and data security and is based largely on the TCDP Concept of Protection Categories.

1 The data protection certification

A central element of the AUDITOR certification mechanism is the criteria catalogue. It converts the normative requirements of the General Data Protection Regulation and the Federal Data Protection Act into verifiable criteria for data processing operations in the context of cloud services. The criteria catalogue focuses on cloud providers in their function as processors pursuant to Art. 4 No. 8 GDPR. In addition, the criteria catalogue also addresses cloud providers as controllers of data processing operations. However, this is only necessary to the extent that the processing operations are necessary in order to conclude and perform the contract with the cloud user on the provision of the cloud service and to the extent that the cloud provider has legal obligations to carry out data processing, which may be the case, for example, with recording and retention obligations under commercial and tax law.

For some criteria, the criteria catalogue makes a distinction according to protection categories and defines different requirements that must be met. Protection categories are an important tool in data protection certification because they can be used to express the individual protection needs of data processing operations and their fulfilment through certified cloud services. The basic principles and design of the protection categories are described in this Concept of Protection Categories.

The certification object of the AUDITOR certification are the data processing operations in the context of cloud computing performed in products or services or with the help of (several) products or services. Since data processing operations or bundles of data processing operations are regularly in the form of services, this document often makes use of the term “certification of cloud services”. However, this does not change the fact that this term always refers to the certification of data processing operations in the context of cloud computing because Art. 42 para.1 sentence1 GDPR defines data processing operations as the object of the certification.

Pursuant to Art. 28 para.1 GDPR, the cloud user as the controller of data processing may only use such cloud providers as processors “providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation […]”. Art. 28 para. 5 GDPR states that controllers may use processors’ successfully completed approved certification mechanisms as an element by which to demonstrate sufficient guarantees of the processor as referred to in Art. 28 para. 1 GDPR.

Where the cloud provider has undergone an approved certification mechanism and meets the criteria relevant to the cloud provider, it shall receive a certificate from the accredited certification body carrying out the certification. In this case, the cloud user may rely on the fact that the certified cloud service is offered in a data protection-compliant manner and does not have to check the technical and organisational measures of the selected cloud provider itself and satisfy itself of them.

2 Consideration of individual data protection and data security requirements through protection categories

2.1 Certification and risk-based approach for technical and organisational measures in data protection and data security

An AUDITOR certificate informs the cloud user whether a cloud provider fulfils all the normative requirements of the General Data Protection Regulation and the Federal Data Protection Act for its cloud service. An essential element of the legal requirements are the technical and organisational measures to be taken by the cloud provider to comply with the central data protection principles under Art. 5 para.1 GDPR.

In the Standard Data Protection Model, the Conference of the Independent Data Protection Authorities of the German Federation and the German States has formulated so-called protection goals for requirements for legally compliant data processing that result from data protection law and that can and must be guaranteed by technical and organisational measures. They are: data minimisation, availability, integrity, confidentiality, unlinkability, transparency, and intervenability.

The technical and organisational measures that cloud providers must take to meet the protection goals in the event of using AUDITOR are not prescribed by the General Data Protection Regulation in any generally valid and absolute form. Rather, the so-called risk-based approach laid down in Art. 24, 25, and 32 GDPR requires that the measures must always be selected in accordance with the specific circumstances of the processing and the risks associated with the processing for the rights and freedoms of the data subjects. Specifically, the General Data Protection Regulation stipulates in Art. 32 para.1

GDPR, e.g. with regard to the security of processing, that the requirements for the technical and organisational measures, and thus also the degree of reliability of these measures to be achieved, must be determined by "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". The measures must therefore "ensure a level of security appropriate to the risk".

Explanatory note: The Federal Office for Information Security (BSI) also refers to the Standard Data Protection Model in section "CON.2 Data Protection" in No. 3.1 of its IT Basic Protection (IT-Grundschutz) and demands that the failure to take into account the complete catalogue of protection objectives and not to apply this methodology and the reference measures must be justified. Cloud providers must therefore also deal with the Standard Data Protection Model within the framework of the ISO 27001 certification on the basis of the IT-Grundschutz.

2.2 Concept of Protection Categories

The protection level is expressed in the Concept of Protection Categories by different "protection categories". The cloud user of a cloud service can classify the individual protection needs of its data processing operations into the appropriate protection category and choose a cloud service for which the data protection and data security level corresponds to the protection category it requires. The cloud user can find the protection category of a cloud service in the cloud provider's certificate.

The protection category has a dual role: On the one hand, it describes the protection needs of data processing operations. On the other hand, it defines the technical and organisational requirements that the cloud provider must meet.

So as to make this dual role clear, the protection category distinguishes two components: the categories of protection needs and the categories of protection requirements. The category of protection needs describes the protection need for data processing operations on the basis of general characteristics. The category of protection requirements describes the technical and organisational requirements that the cloud provider must fulfil for cloud services of the relevant category in general terms. For each category of protection needs, a corresponding category of protection requirements is defined.

It is not necessary to assign each legal requirement (in the form of the criteria in the AUDITOR criteria catalogue) to a particular category of protection requirements since the non-technical-organisational data protection requirements for processing are independent of the protection need. For example, the obligation of the cloud provider to assist the cloud user in responding to requests for exercising the data subject's rights laid down in Art. 28 para. 3 lit. e GDPR constitutes a statutory requirement for processing, which, however, is independent of the protection need of the respective data processing operation.

However, different normative requirements must be formulated where a different protection need leads to different requirements for technical and organisational measures. The criteria catalogue formulates criteria dependent on the protection category, above all in Chapter II No. 2, on the guarantee of data security.

Although the formation of categories of protection needs goes hand in hand with generalisation, the Concept of Protection Categories must ensure that the individual protection need of data processing is covered by technical and organisational requirements of the category of protection requirements in question. This is achieved in the Concept of Protection Categories by defining the protection requirements in such a way that they cover the highest individual protection need in the corresponding category of protection needs.

This ensures that sufficient protection requirements apply to all individual protection needs in the respective category of protection needs. At the same time, this has the consequence that in many cases higher protection requirements are made in the categories of protection requirements than would be necessary according to the individual protection needs of data processing. The cloud provider of a certified cloud service will therefore often meet a higher level of protection requirements than would be required by the individual legal requirements of the data processing operation.

2.3 Mapping individual protection needs through categories of protection needs

2.3.1 Requirements of categories of protection needs

The prerequisite for certification according to protection categories is that each individual protection need can be assigned to a category of protection needs. The categories of protection needs are therefore defined in such a way that they completely cover every individual protection need. For this purpose, they are described with characteristics that reflect the protection needs of the specific data processing operation. The description enables the controller of data processing to assign the protection need of its data processing to the characteristics of the protection category.

For data security, the protection need pursuant to Art. 32 para.1 GDPR is determined on the basis of several factors: In particular, the general sensitivity of the data according to its type, the scope of data processing, the context, and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing are decisive. According to Art. 32 para.2 GDPR, "in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". When determining the category of protection needs, the specific processing must therefore always be taken into account. Since all relevant circumstances have to be taken into account – and therefore sometimes a multitude of circumstances – determining the specific protection need can become complicated. However, this does not prevent the formation of protection categories.

If, for example, a cloud user processes data such as the personal identification number or the transaction number in online banking, the cloud user must in particular deal with attacks by unauthorised persons, the abuse of this data, and the probabilities of these incidents because this data offers access to economic advantages and therefore arouses particular interest.

2.3.2 Steps for ascertaining the protection need of data processing operations

Since a merely general description of the protection need bears the danger that assigning the individual protection need to a category of protection needs is solely dependent on the assessments of the respective controller and is therefore very subjective – which can lead to legal uncertainty and impair the benefit of certification – the Concept of Protection Categories contains a system for determining the protection need.

Ascertaining the protection need is always the responsibility of the controller processing the data pursuant to Art. 4 No.7 GDPR. For data processing operations with content and application data that is transferred to the cloud and processed there, the cloud user is the controller and must therefore ascertain the protection need. For data processing operations performed by the cloud provider to provide the cloud service and to enable its use and invoicing (processing of personal information and usage data) or to comply with legal obligations, it is the cloud provider's responsibility to determine the protection need.

The starting point and first step is ascertaining the abstract protection need based on the type of data. It is a recognised fact that the type of the data processed has a significant impact on the protection need of data processing because certain types of data, such as health-related data, have a much greater impact on the personal rights of the data subject than other types of data.

In a second step, it must be checked whether circumstances exist that increase the protection need and whether the protection need increases to such an extent as a result of these circumstances that it is necessary to upgrade to a higher category of protection needs.

The upgrade will normally concern one category of protection needs. In some cases, an upgrading by two categories of protection needs can also be considered. The intermediate result of this audit shall be a classification of the data processing operation into a category of protection needs.

The third step is for checking whether circumstances exist that reduce the protection need. They can lead to the data processing operation being assigned to a lower category of protection needs as a result than would be the case after the intermediate result of the second step. The possibility of downgrading arises from the fact that the law requires all circumstances of the individual case to be decisive. An example of a circumstance that lowers the protection need is the prior encryption of content and application data by the cloud user before it is transmitted to the cloud provider and stored in a host service. As per the upgrade of the protection need in the second step, a downgrade by one or more categories of protection needs may be necessary. At the end of the third step, the category of protection needs relevant for the respective data processing is determined.

If multiple data processing operations are to occur in a cloud service, the service must meet the protection need of all data processing operations. Therefore, the selection of the service is ultimately based on the highest protection need required by the various data processing operations.

In practice, identifying the category of protection needs relevant to a data processing operation may be difficult. In these cases, the controller can, when in doubt, protect itself by choosing the higher category of protection needs in order to avoid risks.

2.4 Categories of protection requirements for technical and organisational measures

In accordance with the objective of the Concept of Protection Categories, corresponding protection requirements must be defined for each category of protection needs that fulfil the protection requirement and are defined in the categories of protection requirements.

The protection requirements are described using abstract characteristics so that they can be fulfilled by various technical and organisational measures. When designing its cloud service, the cloud provider may choose the measures that it will take in view of the different categories of protection requirements. As part of the certification of the cloud service, the measures are checked whether they meet the requirements of a certain category of protection requirements. If this is the case, the certificate will be issued for the corresponding protection category.

The technical and organisational requirements cannot be assigned by means of a catalogue. As such it is not possible to, for example, assign the protection need to a specific category of protection requirements as part of access protection by a blanket password since the use of passwords must satisfy very different security requirements depending on the design and circumstances of the individual case. In this respect, there is a considerable need for interpretation, which includes the assessment of all circumstances of the specific design of the service. This evaluation is carried out during the certification as part of the audit. It is therefore necessary that the auditing and certification be carried out by qualified auditor and accredited certification bodies.

As in the case of the categories of protection needs, it must also be noted for categories of protection requirements that a differentiation according to categories of protection requirements is not required for every legal requirement for order processing because legal requirements are often independent of protection needs.

2.5 Number of protection categories

The AUDITOR Concept of Protection Categories comprises three protection categories. Each of them describes protection needs (categories of protection needs) and protection requirements (categories of protection requirements).

Three protection categories are formed because sufficiently different requirements can be defined for this number, and a stronger differentiation would be too great a difficulty in clearly assigning measures to categories of protection requirements. The differentiation of three protection categories represents the minimum degree of differentiation because having only two protection categories would run the risk of requirements often having to be met that are considerably higher than the individual protection need and thus would incur costs that are not justified by the actual protection need. Three protection categories make the certification manageable for cloud providers and cloud users because the assignment of an individual protection need or protection measure to a protection category is made simple and unambiguous.

Data processing operations that do not provide – nor generate, assist, or enable – an indication of personal or factual affairs of natural persons do not have any protection needs under data protection laws. Because no personal data is processed, these data processing operations are below protection category 1, which is why they are omitted from the Concept of Protection Categories.

Example: The cloud user wants to process raw weather data, effectively anonymised data, or synthetically generated test data (“John Doe”).

Data processing operations with an extremely high protection need (above category of protection needs 3) are omitted from the Concept of Protection Categories and the AUDITOR certification. There is an extremely high need for protection when, on the basis of the data used or the actual processing of such data, the data processing operations have, can support, or lead to a critical informative value concerning the personality or circumstances of the data subject or are otherwise of considerable importance for the circumstances of the data subject, and when the unauthorised processing of such data would lead to a concrete risk of substantial impairment of the life, health, or freedom of the data subject.

Example: The cloud user wants to store data from undercover informants of the Federal Office for the Protection of the Constitution or data on persons who may be potential victims of criminal offences. The unauthorised disclosure of such data could lead to danger to life and limb of the data subjects.

Data processing operations with individually strongly diverging circumstances are also not considered in the Concept of Protection Categories and the AUDITOR certification because they are not accessible to the generalization associated with the Concept of Protection Categories.

If data processing operations have extremely high protection needs or widely diverging circumstances, the cloud user who wishes to outsource its data processing to a cloud provider must in this case carry out a risk analysis itself and, on the basis of this analysis, determine the requirements for the technical and organisational measures of the cloud provider and ensure that the requirements of the cloud provider are met because the AUDITOR certificate is only issued for protection categories 1, 2, and 3.

2.6 Application of the Concept of Protection Categories in the certification and use of cloud services

The application of the Concept of Protection Categories in the certification and use of cloud services leads to a differentiated distribution of tasks between the cloud provider and the cloud user as well as the accredited certification body.

The cloud user assigns the protection need of its specific data processing operations to a specific category of protection needs. The cloud user determines the protection need based on the three steps described above and can then choose a cloud service that is certified for the protection category in question.

The cloud provider guarantees a certain category of protection needs when processing data and applies for a certification for the corresponding category of protection requirements. The cloud provider is also responsible for determining the category of protection needs for data processing operations that the cloud provider performs to enter into and perform the contract on the provision of the cloud service with the cloud user or to fulfil legal obligations.

The accredited certification body assigns the cloud service to a specific protection category using technical and organisational measures, based on the audit conducted as part of the certification mechanism. The certificate shows the suitability of the cloud service for a specific category of protection requirements.

3 Protection categories

Below, the categories of protection needs are defined and explained using examples (3.1). Subsequently, the assignment of the protection need of a data processing operation to a category of protection needs is presented using the three-step process (3.2). First, the abstract categories of protection needs are defined according to the respective data type (3.2.1), and then factors are presented that lead to an upgrading (3.2.2) or downgrading of the protection need (3.2.3). Lastly, the categories of protection requirements are described (3.3).

3.1 Categories of protection needs

3.1.1 Category of protection needs 1

Any processing of personal data constitutes an interference with the fundamental rights of the data subject. For this reason, it is assumed that any processing of personal data involves at least a normal protection need.

Category of protection needs 1 includes all data processing operations that, due to the data entered and the specific processing of this data contain, generate, assist or enable statements about the personal or factual affairs of the data subject. The unauthorised use of this data can easily be prevented or ceased by the data subject through taking action or does not result in any specific impairments for the data subject.

Explanatory note: For the data subject to be able to take action against data processing, he or she must be given information about the data processing and be able to exercise his or her other data subject rights under Art. 17–22 GDPR. How easy it is to exercise data subjects' rights depends to a large extent on the specific design of the cloud service.

Example: The cloud user wants to store and manage the address data of its contracting parties. This data processing operation includes information about the contracting parties' personal affairs due the type of the data (name, gender, address).

3.1.2 Category of protection needs 2

Data processing operations that, due to the data used or the specific processing of these data are capable of providing or sustaining informative value about the personality or the life of the data subject or that could lead to such information or that are otherwise of significance to the data subject's affairs. The unauthorised processing of such data may lead to impairments to the social status or the economic circumstances of the data subject ("reputation"). In addition, data that were identified as particularly worthy of protection by the legislator in Art. 9 para. 1 GDPR must be presumed to have a high protection need.

Example: The cloud user (employer) wants to process the degree of disability of employees in question. This data processing operation includes information about the employees' health due to the type of the data and the processing, therefore requiring a high protection need.

3.1.3 Category of protection needs 3

Data processing operations that, due to the data used or the specific processing of these data are capable of providing or sustaining considerable informative value about the personality or the life of the data subject or that could lead to such information or that are otherwise of considerable significance to the data subject's affairs. The unauthorised processing of such data may lead to considerable disadvantages for the data subject regarding its social status and its economic circumstances ("livelihood").

Example: The cloud user is a lawyer and wants to process client data that is subject to lawyer-client privilege.

3.2 Ascertaining the protection need

Determining the protection need for content and application data is the cloud user's responsibility. For data processing operations for which the cloud provider acts as the controller, the cloud provider must also ascertain the protection need. The protection need is always ascertained in a three-step process:

- In step 1, the abstract protection needs of the data to be processed are determined based on the data type.
- In step 2, it must be checked whether the protection needs are increased due to the specific use of the data.
- In step 3, it must be checked whether the protection needs decrease due to specific circumstances.

The protection needs of the specific data processing activity are then classified in one of the categories of protection needs.

3.2.1 Categories of protection needs per data type (step 1)

In step 1, the abstract protection needs of the data to be processed are determined based on the data type.

3.2.1.1 Data types with a normal protection need (category of protection needs 1)

Personal data within the meaning of Art. 4 No.1 GDPR, i.e. any information relating to an identified or identifiable natural person and which is unlikely to result in any specific impairments to the rights and freedoms of the data subject.

Non-exhaustive examples of data (without a processing context, as long as not in category of protection needs 2 or 3):

- Name;
- Gender;
- Address;
- Profession;
- Year of birth;

- Title;
- Address book information;
- Telephone records;
- Nationality;
- Telephone number of a natural person.

3.2.1.2 Data types with a high protection need (category of protection needs 2)

Data that has a specific informative value about the personality or the life of the data subject or is otherwise of significance to the data subject’s affairs. The unauthorised processing of such data may lead to impairments to the social status and economic circumstances of the data subject (“reputation”).

The category of protection needs 2 also includes data types that the legislator has designated as being particularly worthy of protection in Art. 9 para.1 GDPR.

Non-exhaustive examples of data (without a processing context, as long as not in category of protection needs 3):

- Name, address of a contracting party;
- Date of birth;
- Marital status;
- Family relations and acquaintanceships;
- Data on business and contractual relationships;
- Context on a contractual partner (e.g., subject-matter of an agreed service);
- Processing of non-changeable personal data that can serve as lifelong anchors for profiling such as genetic data within the meaning of Art. 4 No.13 GDPR or biometric data within the meaning of Art. 4 No.14 GDPR.
- Data on racial and ethnic origin;
- Data on political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data on a natural person’s sex life or sexual orientation;
- Processing of clearly identifiable, highly linkable data such as health insurance numbers or tax numbers;
- Data that have potential effects on the standing/reputation of a data subject;
- Data about the protected inner life of the data subject (e.g., diaries);
- Data concerning health within the meaning of Art. 4 No.15 GDPR
- Degree of disability;
- Processing data with inherent lack of transparency for the data subject (estimated values for scoring, application of algorithms);
- Income;
- Social benefits;
- Taxes;
- Administrative offences;
- Data on rental agreements;
- Patient administration data (with the exception of particularly sensitive diagnostic data and the like);
- Work time data;
- Membership directories;
- Civil register;
- Certificates and exam results;
- Insurance data;
- Personnel administration data from employment relationships (with the exception of company assessments and professional career);
- Traffic offences;
- Simple evaluations of little importance (e.g., yes/no decision for classification in a mobile phone contract, etc.);
- Access data for a service;
- Content of communication with a person (e.g., email content data, letter, telephone call);
- (Exact) location of a person;
- Financial data about a person (e.g., account balance, credit card number, individual payment);

- Credit reports;
- Telecommunications traffic data.

Explanatory note: Communication contents, especially written or audio recordings of all types, can have very different protection needs, from low to very high. Determining the protection need requires an objective assessment in which the extent of the risk of data processing is evaluated. If the cloud user has no knowledge of the subjective protection need of the communicating party (e.g., general collaboration service with data storage, video conference and mail function) or offers its services for communication that is particularly worthy of protection (e.g. conference service for lawyers and clients, here: protection category 3) it may assume the category of protection needs 2.

3.2.1.3 Data types with a very high protection need (category of protection needs 3)

Data that has a considerable informative value about the personality or the life of a data subject or is otherwise of considerable significance to the data subject's affairs because the data is, for example, directly dependent on the decision or performance of the data processor in an existential way. The unauthorised processing of such data may lead to considerable disadvantages for the data subject regarding its social status and its economic circumstances ("livelihood").

Explanatory note: Data types in this sense also include data majorities, in particular linked data (e.g. personality profiles) that result in new information content.

Non-exhaustive examples of data with very high protection needs:

- Data subject to professional, business, telecommunications or client secrecy (e.g., patient data, client data);
- Data of which the knowledge enables significant specific harm to the data subject or third party (e.g., personal identification number, transaction number in online banking);
- Debts;
- Particularly sensitive social information;
- Seizures;
- Personnel administration data such as company assessments, professional careers, and the like, as long as not in category of protection needs 2;
- Data about previous convictions and circumstances related to criminal proceedings (e.g., preliminary proceedings) of a person and corresponding suspicions, delinquencies;
- Particularly sensitive data concerning health within the meaning of Art 4 No. 15 GDPR, such as data about illnesses, the knowledge of which is unpleasant to the data subject to a particular extent, or which could lead to social stigmatisation of the data subject;
- Personality profiles, e.g., movement profile, relationship profile, interest profile, purchase behaviour profile, with considerable informative value about the personality of the data subject.

3.2.2 Upgrading (step 2)

The protection need of data processing may increase as a result of various circumstances if the circumstances are likely to result in a greater impairment to the personal rights of the data subject. In this case, the data must be classified into a higher category of protection needs.

It should also be noted that if the protection need increases as a result of the circumstances listed below, the risk of abuse will also regularly increase, as this is determined not only by the type of data but also by the circumstances of the data processing.

Example: Storing a large amount of credit card information in one place can make this data a worthwhile target for criminals; so the risk of abuse increases due to the fact that data is processed in large quantities. After all, accessing a large amount of credit card information is more "rewarding" for criminals than just accessing a small amount of data. The threat to all stored credit card information is increased.

Circumstances that can lead to an upgrading are, in particular:

- Context of use of data;
- Linking of data;
- Quantity of data;
- Number of data subjects;
- Accumulation of many rights;
- Automated decision-making;

- Use of highly complex and highly networked technology;
- No control possibilities for data subjects.

→ Context of use of data

The context of use of data may lead to a greater protection need if this is accompanied by a considerable increase in the informative value of the data relating to the personality of the data subject or if the unauthorised use may have specific disadvantages for the data subject.

Example: The use of the name in a (general) telephone directory does not normally establish an increased informative value. The use of the name in the patient list of a physician does establish this, however, potentially even considerably.

Context of use **examples** that increase the protection need are:

- Data type: Name, address;
- Context of use: Certificate of good conduct; criminal photo file, criminal records, employee screening, personnel file.

→ Linking of data

The linking of data means the combining of data with other data in order to obtain new meaning. Linking can lead to a greater protection need if this is accompanied by a considerable increase in the informative value of the data relating to the personality of the data subject. This also applies if one data set is linked with other data of the same or a lower category of protection needs.

Example: The combination of data on the purchase of products (category of protection needs 2) and, if necessary, other data of the same or a different type, such as a person's location (category of protection needs 2), can lead to an exact personality profile depending on the amount of data. Such a personality profile can be classified as category of protection needs 3.

Examples of data that can be linked to increase protection needs are:

- Location data that can be combined into a specific movement profile (the combination is possible and obvious in the specific situation).

→ Quantity of data

The sheer volume of data alone can lead to an increased interest in unauthorised processing of data; thus, there is a higher risk of unauthorised processing also with regard to individual data. The protection need of data can increase on account of it being processed in larger quantities.

Example: Storing a large amount of credit card information in one place can make this information a worthwhile target for criminals, increasing the likelihood of an attack. This increases the risk for all credit card information stored there.

Examples of the combination of data that increases the protection need are:

- Collection of large amounts of bank and credit card information.
- Collection of data from video surveillance systems

→ Number of data subjects

A large amount of data is often accompanied by a large number of data subjects. However, a need to increase protection can also arise where large amounts of data are not processed but a large number of data subjects are affected by the processing.

→ Accumulation of many rights

Furthermore, the protection need of data may increase if it is processed by persons who, for different purposes, perform different roles with different rights, thus increasing the level of control over the data held by these persons.

Example: The administrator of an online service gets a comprehensive picture of the data subject whose data he or she manages due to the multitude of the rights he or she has.

→ **Automated decision-making**

The protection need of data may also increase if the processing of data is intended to lead to automated decision-making that produces legal effects vis-à-vis the data subject or that similarly significantly affects the data subject without him or her being able to have any influence on the decision.

Example:

The applicants for a vacant position are automatically pre-selected by algorithms without a personnel clerk checking the selection.

→ **Use of highly complex and highly networked technology**

The protection need for data can also increase if a highly complex and highly networked technology is to be used during processing because the networking of the individual components creates additional attack possibilities for cyber-attacks. In addition, networked technology often encompasses different areas of its users' lives and therefore provides information with a very high informative value about the personal life and factual affairs of these data subjects, the unauthorised access of which can result in serious disadvantages for them.

Example: Smarthome applications can consist of many data processing components such as smart motion detectors, surveillance cameras, heating and air conditioning, access and elevator controls. Unauthorised access to data from motion detectors provides information about the presence of residents and can serve as a basis for planning burglaries.

→ **No control possibilities for data subjects**

The protection need for data may further increase if the data subject is not given an opportunity to exercise direct control over his or her data so that the data processing operations do not provide any means of intervention or self-protection possibility for the data subjects.

3.2.3 Downgrading (step 3)

The protection need of data processing may be decreased as a result of various circumstances in so far as the circumstances or certain measures reduce the risk of interference or the informative value of the data. Depending on the extent of the protection need achieved, the decreased protection need can lead to a classification into a lower category of protection needs.

Example: With (effective) pseudonymisation of the data, the informative value for anyone who does not know the classification rule is significantly reduced. Circumstances that can lead to a downgrading are, in particular:

- Information content and context of use;
- Encryption of personal data (Art. 32 para.1 lit. a GDPR);
- Pseudonymisation of personal data (Art. 4 No. 5 and Art. 32 para. 1 lit. a GDPR);

Explanationory note: Encryption and pseudonymisation of data are both measures used to protect personal data. Encryption as well as pseudonymisation have a double meaning: From the view of the cloud provider, they influence the protection need of data. For example, data requires a lesser protection need if it is made available to the cloud provider in a pseudonymised or encrypted form. Irrespective of this, encryption and pseudonymisation are among the measures that the cloud provider can use to protect data against unauthorised access.

→ **Information content and context of use**

Due to their information content and the context of use, data may have less informative value about the personal or factual affairs of the data subject than what corresponds to the abstract classification of the data type.

Example: A patient's appointment with a family doctor or dentist must be classified as data concerning health. Because the mere information on an appointment does not have any significant informative value with regard to the personality and/or life of the data subject, the protection need corresponds to other location data. However, this is not the case with an appointment with a specialist (e.g. oncologist) because this enables considerable conclusions to be drawn about possible illnesses of the data subject.

→ **Data encryption**

The encryption of data changes personal data in such a way that without decryption it is not possible or only possible with disproportionately high effort to know the content of the data.

Explanationory note: The encryption of data only reduces the protection need if it is carried out by the cloud user before the data is transferred to the cloud provider. This encryption must therefore be differentiated from the encryption of stored data as a protection requirement according to No. 2.9 of the AUDITOR criteria catalogue.

→ **Data pseudonymisation**

Pseudonymisation means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Art. 4 No. 5 GDPR).

Explanatory note: The pseudonymisation of data only reduces the protection need if it is carried out by the cloud user before the data is transferred to the cloud provider. This pseudonymisation must therefore be differentiated from the pseudonymisation as a protection requirement according to No. 2.7 of the AUDITOR criteria catalogue.

3.3 Categories of protection requirements

The categories of protection requirements serve to define the technical and organisational measures that are appropriate to reach the protection goal of the respective protection category, therefore adequately protecting the rights and freedoms of data subjects in relation to the risks of service. The greater the risk, the higher the protection requirement.

In addition to the type of data to be processed, it is important that the definition of the measures also takes into account the technical systems involved (hardware, software, and infrastructure) and their interfaces and the technical and organisational (including staff) processes of processing data with the systems because the systems and processes linked to the specific data processing inherit the protection need for the data.

It is also important that the defined measures must themselves comply with the protection goals.

Example: When storing log data, the logs must be available, protected for integrity, secured against unauthorised access, and subject to a separate purpose limitation.

3.3.1 Category of protection requirements 1

By taking risk-appropriate technical and organisational measures, the cloud provider must ensure data minimisation, availability, integrity, confidentiality, unlinkability, transparency, and intervenability of personal data. For information security, this means that data must be protected against destruction, loss, alteration, unauthorised access, and disclosure in particular, and the resilience of the cloud service must be guaranteed.

As a rule, the measures must be appropriate for excluding such processes due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve. It must be possible to determine each interference at a later date.

Explanatory note: A catalogue of measures for normal protection needs will be made available in the future in the Appendix to the Standard Data Protection Model[1]. The measures should be used as references to mitigate risks and achieve the protection goals. The catalogue of measures is currently being developed. The first components of the Catalogue have been published.[2] They have not yet been agreed on in the data protection conference, however, but are in the trial phase.

[1] The Standard Data Protection Model, V. 1.1 – trial phase, available at: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.

[2] The components can be viewed at e.g. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

3.3.2 Category of protection requirements 2

A high protection need leads to additional or more effective risk-appropriate technical and organisational measures having to be taken in order to ensure data minimisation, availability, integrity, confidentiality, unlinkability, transparency, and intervenability of personal data. For information security, this means that data must be protected against destruction, loss, alteration, unauthorised access, and disclosure in particular, and the resilience of the cloud service must be guaranteed. At the same time, the measures appropriate for category of protection requirements 1 must be fulfilled and their design adapted to the protection need.

A high protection need does not always require the implementation of a multitude of additional measures. In many cases, it suffices to increase the effect of a measure insofar as it provides a starting point for such scaling. The use of longer cryptographic keys, two-factor authentication, or hardware tokens are a few examples. Furthermore, an adjustment can be made by ensuring that the measure is carried out with greater reliability in accordance with the specifications. For this, possible disturbance influences must be determined and the robustness of the measures must be increased by taking additional precautions, which are often organisational ones.

As a rule, the measures taken must be appropriate for excluding such processes due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of third parties. As a rule, the measures must also be appropriate for preventing damage caused by negligent actions of authorised persons. Protection must be provided that rules out expected interference with sufficient certainty. This includes adequate protection against known attack scenarios in particular as well as measures through which interferences can normally be detected (subsequently).

Explanatory note: A catalogue of measures for high protection needs will be made available in the future in the Appendix to the Standard Data Protection Model[3]. The measures should be used as references to mitigate risks and achieve the protection goals. The catalogue of measures is currently being developed. The first components of the Catalogue have been published.[4] They have not yet been agreed on in the data protection conference, however, but are in the trial phase.

3.3.3 Category of protection requirements 3

In addition to the technical and organisational measures of the categories of protection requirements 1 and 2, the cloud provider must achieve risk-approriate technical and organisational measures to protect the data, in particular against destruction, loss, alteration, unauthorised access, and unauthorised disclosure.

The measures must be appropriate for excluding with sufficient certainty such processes due to technical or organisational errors, including operating errors, or due to acts of negligence or intent. This includes sufficient protection against known attack scenarios in particular as well as procedures for identifying abuse. It must be possible to determine each interference at a later date.

[3] The Standard Data Protection Model, V. 1.1 – trial phase, available at: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.

[4] The components can be viewed at e.g. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.