European Cloud Service
Data Protection Certification

AUDITOR Concept of Protection Categories

- Version 0.99 -

Status: 11/27/2019

Related AUDITOR publications:

- certification object
- criteria catalogue
- concept of modularity
- DIN SPEC 27557

Available online: www.auditor-cert.eu

Recommended Citation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier-Reinhardt, N. & Teigeler, H. (2019). AUDITOR Concept of Protection Categories – version 0.99. Online available: www.auditor-cert.eu

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

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-Reinhardt[a], Heiner Teigeler[b]

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

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

Table of contents

List of abbreviations and acronyms

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 the gender-neutral wording:

All references to persons in the AUDITOR Criteria Catalogue shall be considered to be gender-neutral. Therefore, for the purpose of better readability, no gender-specific wording is used, while the male grammatical form shall apply to all genders equally (e.g., any use of the title “data protection officer” in combination with male pronouns is a reference to the functional description as gender-neutral and without specifically referring to a person of the male gender).

Note on AUDITOR as successor to the TCDP:

Certification according to the former 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), which was finalised in September 2016. TCDP represents an audit standard for data protection certification of cloud services according to the former Federal Data Protection Act and distinguishes three protection categories, which are described in the Concept of Protection Categories. As the successor to the TCDP, the research project AUDITOR has developed a standard for data protection certification of cloud services according to the General Data Protection Regulation (GDPR). The AUDITOR Criteria Catalogue also 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 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 testable 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 addresses cloud providers as controllers of data processing operations, which the cloud provider undertakes in order to enter into and perform the contract with the cloud user for the provision of the cloud service and to fulfil legal obligations. Legal obligations exist, for example, in relation to 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 is 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 groups of data processing operations regularly take 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, since Art. 42 para.1 sentence1 GDPR defines data processing operations as the object of certification.

Pursuant to Art. 28 para.1 GDPR, the cloud user as the controller of data processing may only use cloud providers as processors which provide “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 successful completion of approved certification mechanisms by processors as an element by which to demonstrate sufficient guarantees for the processor referred to in Art. 28 para. 1 GDPR.

Where the cloud provider has undergone an approved certification mechanism and meets the criteria relevant to cloud providers, it receives 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 its Standard Data Protection Model, the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder (Data Protection Conference) has formulated 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 if they use AUDITOR are not prescribed by the General Data Protection Regulation in any generally valid or 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, with

regard to the security of processing for example, that the requirements for the technical and organisational measures, and thus also the degree of reliability provided by those measures, 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”.

Note: The Federal Office for Information Security (BSI) also makes reference to the Standard Data Protection Model in section “CON.2 Data Protection” in ”CON.2.A1 Implementing the German Standard Data Protection Model (B)” of its IT-Grundschutz-Compendium and, if the complete catalogue of protection objectives is not taken into account and this methodology and the reference measures are not applied, it requires a justification. Cloud providers must therefore also engage with the Standard Data Protection Model within the framework of ISO 27001 certification on the basis of the IT-Grundschutz-Compendium.

2.2 Concept of Protection Categories

The protection level is expressed in the Concept of Protection Categories in terms of 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 on 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 between two components: the protection needs categories and the protection requirements categories. The protection needs category describes the protection need for data processing operations on the basis of general characteristics. The protection requirements category describes the technical and organisational requirements that the cloud provider must fulfil for cloud services of the relevant category in general terms. For each protection needs category, a corresponding protection requirements category 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 protection requirements category, 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 from data subjects to exercise their 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.

At the same time, different normative requirements must be formulated where a different protection need leads to different requirements of technical and organisational measures. The criteria catalogue formulates criteria according to the protection category in terms of the guarantee of data security, particularly in Chapter II No. 2.

Although the formation of categories of protection needs involves a degree of generalisation, the Concept of Protection Categories must ensure that the individual protection need of data processing is covered by the technical and organisational requirements of the protection category 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 protection needs category.

This ensures that sufficient protection requirements apply to all individual protection needs in the respective protection needs category. At the same time, it means that in many cases higher protection requirements are stipulated in the protection requirements categories 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 to protection needs categories

2.3.1 Requirements of protection needs categories

The prerequisite for certification according to protection categories is that each individual protection need can be assigned to a protection needs category. The protection needs categories 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.

In the area of 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 key factors. 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 protection needs category, the specific processing must therefore always be taken into account. Since all relevant circumstances have to be considered – and therefore a multitude of circumstances in some cases – 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 for online banking, the cloud user must in particular take account of attacks by unauthorised persons, misuse of this data, and the probabilities of these incidents because the data offers access to economic advantages and therefore attracts particular interest.

2.3.2 Steps for ascertaining the protection need of data processing operations

Since a general description of the protection need alone runs the risk that assignment of the individual protection need to a protection needs category is solely dependent on the assessments of the respective controller and is therefore highly subjective – which can lead to legal uncertainty and mitigate the benefit of certification – the Concept of Protection Categories includes a system for determining the protection need.

Ascertaining the protection need is always the responsibility of the controller who is 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 deliver the cloud service, to enable use of and billing for that service (processing of personal information and usage data) and to comply with legal obligations, it is the cloud provider's responsibility to determine the protection need.

The starting point and first step is to ascertain 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 determined whether circumstances exist that increase the protection need and whether, as a result of these circumstances, the protection need increases to such an extent that it is necessary to upgrade to a higher protection needs category.

The upgrade will normally involve one protection needs category. In some cases, an upgrade of two protection needs categories can also be considered. The intermediate result of this determination is classification of the data processing operation into a protection needs category.

The third step is to verify whether any circumstances exist that reduce the protection need. These can lead to the data processing operation being assigned to a lower protection needs category than the category indicated by 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 considered. 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 is the case in consideration of an upgrade of the protection need in the second step, a downgrade by one or more protection needs categories may be necessary. At the end of the third step, the protection needs category relevant for the data processing in question is determined.

If multiple data processing operations are carried out in a cloud service, the service must meet the protection need of all data processing operations. Selection of the service is therefore ultimately based on the highest protection need required by the various data processing operations.

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

2.4 Protection requirements categories for technical and organisational measures

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

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 protection requirements categories. As part of the certification of the cloud service, the measures are checked to ascertain whether they meet the requirements of the specific protection requirements category that the cloud provider is seeking to achieve through certification. 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. In the context of access protection, for example, it is not possible to assign the protection need of a password simply to one specific protection requirements category, 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 essential for the auditing and certification to be carried out by qualified auditors and accredited certification bodies.

As in the case of the protection needs categories, it must also be noted for protection requirements categories that a differentiation according to protection requirements categories is not required for every legal requirement for commissioned data 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 (protection needs categories) and protection requirements (protection requirements categories).

Three protection categories have been created because sufficiently different requirements can be defined for this number, and greater differentiation would involve difficulties in clearly assigning measures to protection requirements categories. The three protection categories represent the minimum degree of differentiation; having only two protection categories would run the frequent risk of requirements having to be met that are considerably higher than the individual protection need, thereby incurring costs that are not justified by the actual protection need. Three protection categories make certification manageable for cloud providers and cloud users because the assignment of an individual protection need or protection measure to a protection category is straightforward 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 law. Since 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 protection needs category 3) are omitted from the Concept of Protection Categories and the AUDITOR certification. A need for such extremely high protection exists 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 about individuals 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 circumstances that differ significantly from one another are also not considered in the Concept of Protection Categories and the AUDITOR certification because they cannot be covered by the generalisations involved in 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 carry out a risk analysis itself and, on the basis of that 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, as 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 differentiation in the assignment of tasks to the cloud provider, the cloud user and the accredited certification body.

The cloud user assigns the protection need of its specific data processing operations to a specific protection needs category. 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 protection needs category when processing data and applies for a certification for the corresponding protection requirements category. The cloud provider is also responsible for determining the protection needs category for the data processing operations that it undertakes in order to enter into and perform the contract with the cloud user for the provision of the cloud service or to fulfil legal obligations.

The accredited certification body assigns the cloud service to a specific protection category in view of the 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 protection requirements category.

3 Protection categories

The protection needs categories are defined and explained using examples below (3.1). Subsequently, the assignment of the protection need of a data processing operation to a protection needs category is presented using the three-step process (3.2). First, the abstract protection needs categories 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 protection requirements categories are described (3.3).

3.1 Protection needs categories

3.1.1 Protection needs category 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.

Protection needs category 1 includes all data processing operations which, in view of the data entered and the specific processing of that 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 stopped by the data subject taking action or does not result in any specific impairments for the data subject.

Note: For the data subjects to be able to take action against data processing, they must be given information about the data processing and be able to exercise their other rights as a data subject under Art.

17–22 GDPR. How easy it is for data subjects to exercise their 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 circumstances because of the type of data (name, gender, address).

3.1.2 Protection needs category 2

Data processing operations which, in view of the data used or the specific processing of that data, are capable of disclosing information about the identity or circumstances of the data subject or that could assist in or lead to the disclosure of such information, or that are otherwise of significance for the data subject's situation. The unauthorised processing of such data may lead to impairments to the social status or economic circumstances of the data subject ("reputation"). In addition, data that is identified as particularly sensitive under Art. 9 para. 1 GDPR must be presumed to have a high need for protection.

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

3.1.3 Protection needs category 3

Data processing operations which, in view of the data used or the specific processing of that data, are capable of disclosing significant information about the identity or circumstances of the data subject or that could assist in or lead to the disclosure of such information or that are otherwise of considerable significance to the data subject's situation. The unauthorised processing of such data may lead to considerable disadvantages for social status and economic circumstances of the data subject ("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 ascertain the protection need. The protection need is always ascertained by means of a three-step process:

- In step 1, the abstract protection needs of the data to be processed are determined on the basis of the data type.
- In step 2, it must be determined whether the protection needs are greater because of the specific use of the data.
- In step 3, it must be determined whether the protection needs are lower because of the specific circumstances.

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

3.2.1 Protection needs categories by data type (step 1)

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

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

Personal data within the meaning of Art. 4 No.1 GDPR, i.e. any information relating to an identified or identifiable natural person 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, if not in protection needs category 2 or 3):

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

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

3.2.1.2 Data types with a high protection need (protection needs category 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").

Protection needs category 2 also includes data types that the legislator has designated as particularly sensitive in Art. 9 para.1 GDPR.

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

- Name, address of a contracting party;
- Date of birth;
- Marital status;
- Family relations and acquaintances;
- Data on business and contractual relationships;
- Context relating to a contractual partner (e.g. object of an agreed service);
- Processing of non-changeable personal data that can serve as a lifelong anchor 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 about the sex life or sexual orientation of a natural person;
- Processing of clearly identifiable, highly linkable data such as health insurance numbers or tax numbers;
- Data with potential effects on the standing/reputation of a data subject;
- Data about the protected internal 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 an 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);
- Data relating to time in employment;
- 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 information);
- Traffic offences;
- Simple reviews 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 of a person (e.g. account balance, credit card number, individual payment);

- Credit reports;
- Telecommunications traffic data.

Note: The content of communications, especially written or audio recordings of all type, can have very different protection needs, from low to very high. The determination of the protection need requires an objective assessment in which the extent of the risk of data processing is identified. If the cloud provider has no knowledge of the subjective protection need of the parties communicating (e.g. general collaboration service with data storage, video conferencing and email function) or if it offers services for communication that has special protection needs (e.g. conferencing services for lawyers and clients, here: protection category 3), it may assume that protection needs category 2 applies.

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

Data that has a considerable informative value about the personality or life of a data subject or is otherwise of considerable significance for 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").

Note: Data types in this sense also include data majorities, in particular linked data (e.g. personality profiles) from which result new information.

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 the knowledge of which may cause significant specific harm to the data subject or a third party (e.g. personal identification number, transaction number in online banking);
- Debts;
- Particularly sensitive social data;
- Seizures;
- HR management data such as professional evaluations, professional career, etc., if not in protection needs category 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 disclosure 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 the data processing may increase as a result of various circumstances that are likely to result in greater impairment of the personal rights of the data subject. In this case, the data must be classified into a higher protection needs category.

It should also be noted that if the protection need increases as a result of the circumstances listed below, the risk of misuse will also usually 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 misuse 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 accessing a small amount of data only. The threat to all stored credit card information increases.

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

- The 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 opportunities 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 in relation to the personality of the data subject or if unauthorised use may have specific disadvantages for the data subject.

Example: The use of a name in a (general) telephone directory does not normally have a particularly high informative value. The use of the name on a doctor's patient list is more informative, however, potentially even considerably more so.

Examples of contexts of use that increase the protection need include:

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

→ **Linking of data**

Linking of data means combining data with other data in order to create new meaning. Linking can lead to a greater need for protection if it is accompanied by a considerable increase in the informative value of the data in relation 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 protection needs category.

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

Examples of data that can be linked with the result of an increase in protection needs include:

- 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; in turn, this means that there is a higher risk of unauthorised processing with regard to individual data. The protection need of data can increase because it is 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 accumulating of data that increases the protection needs include:

- 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, the 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 those persons.

Example:

The administrator of an online service gets a comprehensive picture of the data subject whose data he manages due to the multitude of the rights he 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 significantly affects the data subject in a similar way without any opportunity for the data subject to influence the decision.

Example:

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 of 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 opportunities 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 circumstances of those data subjects and unauthorised access to which can result in serious disadvantages for them.

Example: Smart home applications can consist of many data processing components such as smart motion detectors, surveillance cameras, heating and air conditioning, access and lift 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 opportunities for data subjects**

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

3.2.3 Downgrading (step 3)

The protection need of the data processing may decrease as a result of various circumstances and measures that reduce the risk of interference or the informative value of the data. Depending on its extent, the lower need for protection can lead to classification in a lower protection needs category.

Example: With (effective) pseudonymisation of data, its informative value is significantly reduced for anyone who does not know the rule for allocation. Circumstances that can lead to a downgrade 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);

Note: Encryption and pseudonymisation of data are both measures used to protect personal data. Both encryption and pseudonymisation have a double significance: from the point of view of the cloud provider, they influence the protection need of data. For example, data has a lower 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**

As a result of the information content and context of use, data may have a less informative value about the personal or factual circumstances of the data subject than the abstract classification of the data type suggests.

Example: A patient's appointment with a family doctor or dentist must be classified as data concerning health. Since the mere information that the data subject has an appointment does not have any significant informative value with regard to their personality and/or life circumstances, the protection need corresponds to any other location data. However, this is not the case for an appointment with a specialist

(e.g. oncologist) because this enables considerable conclusions to be drawn about the possible illnesses of the data subject.

→ **Data encryption**

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

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 Protection requirements categories

The protection requirements categories serve to define the technical and organisational measures that are appropriate to reach the protection goal of the respective protection category and that therefore adequately protect the rights and freedoms of data subjects in relation to the risks of the 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), their interfaces and the technical and organisational (including staff) processes of processing data with the systems, as 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 in terms of integrity, secured against unauthorised access, and subject to a separate purpose limitation.

3.3.1 Protection requirements category 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 data 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 to exclude such processes due to technical or organisational errors of the cloud provider or its employees, including operating errors, and due to acts of negligence on the part of third parties. A minimum level of protection must be provided to make intentional interference more difficult. It must be possible to identify each instance of interference at a later date.

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 by the Data Protection Conference, but are in the trial phase.

[1] The Standard Data Protection Model, V. 2.0b, available at: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

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

3.3.2 Protection requirements category 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 data 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 protection requirements category 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 or hardware tokens are 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 disruptive factors must be determined and the robustness of the measures must be increased by taking additional precautions, often of an organisational nature.

As a rule, the measures taken must be appropriate to exclude such processes due to technical or organisational errors of the cloud provider or its employees, including operating errors, or due to acts of negligence on the part of third parties. As a rule, the measures must also be appropriate to prevent damage caused by negligent actions of authorised persons. Protection must be provided that rules out expected interference with sufficient certainty. This includes especially adequate protection against known attack scenarios and measures by means of which interference can normally be detected (afterwards).

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 by the Data Protection Conference, but are in the trial phase.

3.3.3 Protection requirements category 3

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

The measures must be appropriate to exclude such processes with sufficient certainty due to technical or organisational errors, including operating errors, or due to acts of negligence or intent. This includes especially sufficient protection against known attack scenarios and procedures for identifying misuse. It must be possible to identify each instance of interference at a later date.

[3] The Standard Data Protection Model, V. 2.0b, available at: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

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