Trusted Cloud

Trusted Cloud Competence Centre

Working paper – Protection Categories in Data Protection Certification

Nr. 9

“Cloud Computing Legal Framework” working group

For cloud computing to achieve its economic potential in Germany, the legal framework must be designed to allow efficient use of cloud services. A legal framework that accommodates innovation is therefore crucial. The Federal Ministry for Economic Affairs and Energy (BMWi) has therefore established its own working group within the Trusted Cloud Competence Centre to focus on the legal aspects of cloud computing.

Within this “Cloud Computing Legal Framework“ working group, experts from industry, the legal profession and scientific fields are collaborating with representatives from data protection authorities and participants from the Trusted Cloud programme to propose solutions to legal challenges. The working group is headed by Prof. Dr. Georg Borges. Data protection, contract design, copyright law, general liability issues and the risk of criminal liability are some of the themes addressed by the group. A pilot project on the data protection certification of cloud services is also underway. This is designed to promote the legally secure use of cloud computing and maintenance of a high standard of data protection.

Table of contents

I Data protection compliance certification

In the area of data protection certification, protection categories are an important practical instrument for addressing and fulfilling individual security needs or protection requirements through certified services.

Data protection certification of data processing services is intended to provide legal certainty to the users of such services. The user of a data processing service (such as a cloud service), who avails of this service on an outsourced data processing basis, is considered to be the responsible party under data protection law and as such is obliged to exercise care in selecting the service provider and ensure that the provider meets legal requirements, particularly those relating to technical and organisational measures to guarantee security.

The associated obligation to carry out an inspection on the processor (service provider) is made considerably easier if the relevant service has been awarded a data protection compliance certificate (attestation) by a suitable certification body, where this certificate covers the data processing carried out by the user. This paper uses the term “data protection certificate“ for the certificate or attestation.

In this case, users can trust the certificate and do not themselves have to verify the quality of technical and organisational measures themselves. The proposition paper produced by the “Cloud Computing Legal Framework“ working group describes the elements of this type of data protection compliance certification for cloud services. The pilot project “Data Protection Certification for Cloud Services” elaborates the key principles of the certification, in particular the “Trusted Cloud Data Protection Protocol for Cloud Services (TCDP)“ and general requirements for certification. The EU General Data Protection Regulation (DSGVO) is expected to include a statutory provision on certification that addresses this concept’s basic concern. The concept of data protection certification is not restricted to cloud computing and the provision on certification in the EU General Data Protection Regulation will apply to all data processing services. Certification is of particular relevance in the case of cloud services: cloud services are generally offered as standardised services for multiple users, usually a very large group of users. The efficiency and economic advantages offered by certification are especially vital in the case of these standardised services.

The following section explains the meaning of protection categories under the heading of data protection certification (2.) and then describes the protection categories used as part of the protection category concept (3.).

II. Addressing individual data protection and security requirements using protection categories

1. Certification and individual standards for data protection and security

Data protection certification is centred around a certificate issued by a certification body for a particular data processing service, such as a cloud computing service.

This certificate is designed to inform the service user that the particular service required for data processing purposes meets the applicable requirements in terms of the technical and organisational measures.

The certificate therefore includes a statement by the certification body that a particular service, such as a cloud service, meets the requirements on the part of the processor in relation to outsourced data processing under data protection law. The technical and organisation measures that must be put in place by the processor to ensure IT security form an essential component of the legal requirements.

A key challenge faced by the certification process is that the legal requirements (Section 9 Federal Data Protection Act) of the technical and organisational measures are individual standards: The requirements to be fulfilled by the technical and organisational measures depend on the protection requirement of the particular data processing operation. However, the data processing operation in question and the associated individual protection requirement are not defined by the service provider, or cloud service provider for example, but by the service user, or cloud service user for example.

Since certification must be in place before the service is used by the provider and not only offered to one specific user, but to all potential future users of the service, it cannot refer to one specific data processing operation for a particular user.

2. The protection category concept

This problem can be solved by means of a protection category concept. Under a protection category concept, a service is assessed for its suitability to meet a particular level of security specifications as defined by a protection category. This suitability is then stated in a certificate. A service user can categorise its individual protection requirements according to the protection categories and select a service that complies with the data protection and security level of the protection category it requires.

The protection category thus performs a dual function. First, it describes the protection requirement of the data processing operations. Second, it defines the requirements that must be fulfilled by the technical and organisational measures implemented by the service provider.

To highlight this dual function, this paper distinguishes between protection requirement categories and protection specification categories.

The protection requirement category describes the protection requirement or information security needs for data processing operations on the basis of general characteristics.

The protection specification category describes in general terms the technical and organisational requirements applicable for the data processing services in the relevant category. A corresponding protection specification category is defined for each protection requirement category.

It is not necessary, in this regard, to assign each and every legal requirement to a particular protection specification category. Under data protection law, outsourced data processing is subject to multiple requirements that are independent of the protection requirement. For example, the obligation on the processor to adhere to the instructions of the client is a general legal requirement in relation to outsourced data processing and is largely independent of the protection requirement of the particular data processing operation.

It is the case, rather, that different specifications must be formulated if a different protection requirement places different demands on technical and organisational measures.

A protection category concept must ensure that the individual protection requirement of a data processing operation is covered by the technical requirements of the relevant protection specification category.

To achieve this goal in spite of the generalised approach associated with creating protection requirement categories, protection specification categories must be defined such that they cover the highest individual protection requirement in the corresponding protection requirement category.

In this case, the concept ensures that adequate protection specifications apply for all individual protection requirements in the relevant protection requirement category. At the same time, this approach also means that higher protection requirements often apply than are actually demanded by the individual protection requirement of a data processing operation. As a result, the provider of a certified service will thus regularly fulfil a higher level of protection specifications than required by the individual data processing operation under law. However, the likelihood of this happening is greatly reduced by the formulation of multiple protection categories with differing requirements.

In creating protection categories, it must be ensured that a sufficient degree of protection is established for each individual protection requirement when the service fulfils the requirements of the relevant protection specification class.

3. Representing individual protection requirements with protection requirement categories

a. Criteria for protection requirement categories

A prerequisite for certification based on protection categories is that each individual protection requirement must be capable of being assigned to a protection requirement category.

This assignment is basically possible. Essentially, protection requirement categories must be defined so that they cover each individual protection requirement and that no gaps remain. Furthermore, the protection categories must be described using characteristics that reflect the protection requirement of the specific data processing operation.

The description must allow the service user to assign the protection requirement for its particular data processing operation to the characteristics of the protection category.

The protection requirement of data processing operations is considered to be the starting point for defining the protection requirement categories. This is determined according to Section 9 Federal Data Protection Act on the basis of several factors. A key consideration here is the general sensitivity of the data, depending on the data type, and also any circumstances that would either increase or reduce the protection requirement of the data processing operation. Risks such as the likelihood of unauthorised access or improper use of data are especially significant. Passwords, for example, are particularly at risk if they enable access to economic assets as in the case of PIN and TAN in online banking. Experience has shown that these passwords are subject to higher levels of attack.

For this reason, an individual protection requirement must be defined for each data processing operation, based on the data type and other circumstances. An array of circumstances may quite possibly be relevant, thus resulting in a complex definition of the specific protection requirement.

However, this does not present an obstacle to the establishment of protection categories. The only prerequisite is that each individual protection requirement must be capable of being assigned to a particular protection requirement category. In this regard, the ability to take all applicable circumstances for determining the individual protection requirement into account is vital, as well as the availability of comprehensive protection requirement categories. The former can always be taken for granted, provided that the protection requirement of the protection requirement category is described in general terms.

If the protection requirement is described in purely general terms, assignment of the individual protection requirement to a protection category risks being dependent on the assessments of individual users of the service, which can vary. This can result in considerable legal uncertainty and prevent proper use of the certification.

Example: The user of a cloud service must decide which protection requirement belongs to the data processing operation it wants to perform in a cloud service.

The protection category concept therefore also contains a classification procedure for determining the protection requirement. This classification procedure is designed to represent the theoretical and multidimensional process of determining the individual protection requirement using the relevant factors as a simplified procedure that can be put into practice. The procedure can be simplified because the individual protection requirement does not need to be defined precisely for the purposes of data protection certification. It is simply necessary to determine the applicable protection category.

b. Steps for determining the protection requirement of a data processing operation

The first step in the classification system is, as generally required for determining the protection requirement, to identify the abstract protection requirement based on the data type. It is recognised that the type of data being processed has a major influence on the protection requirement of the data processing operation, since certain data or data types, such as health-related data, can have a significantly greater influence on the personal rights of the affected party.

The second step is to check whether circumstances are present that increase the protection requirement and if so, whether the increase in the protection requirement is sufficient to warrant upgrading to a higher protection category.

Upgrading generally involves just one protection requirement category. However, upgrading by two protection categories may also be considered. As an interim step in this check, the data processing operation must be classified in a protection requirement category.

The third step is to check whether circumstances are present that increase the protection requirement. If so, these can result in the data processing operation being assigned to a lower protection requirement category than would be the case after the interim result in the second step. The option of downgrading the protection requirement category arises from the applicability of all circumstances relating to the individual case, required under the law. One example of a particular circumstance that would reduce the protection requirement is the existence of previously encrypted data that are to be stored in a host service.

This third step also does not require a specific definition of the individual protection requirement of the data processing operation. Instead, the priority is to focus on whether downgrading of the protection requirement should apply due to circumstances that reduce the protection requirements. Based on the downgrading of the protection requirement in the second step, downgrading by one or more protection requirement categories may be necessary at this stage.

The applicable protection requirement category for the data processing operation is defined once the third step is complete.

If several data processing operations are to be carried out within a single service, the service must comply with the protection requirements of all data processing operations. Therefore the highest protection requirement of the various data processing operations is a key factor in selecting the appropriate service.

In practice, it may sometimes be difficult to determine the protection requirement category that applies to a particular data processing operation. In these cases, the data processing operator can take the safe option, when in doubt, by selecting the higher of protection requirement categories under consideration.

Example: A cloud service user is not sure whether its data processing should be classified under protection requirement category 1 or 2.

To avoid the risk of incorrect classification, the cloud service user should assume that the higher protection requirement category 2 applies.

c. Summary: Determining the applicable protection requirement category

The protection requirement of a specific data processing operation is determined using a three-stage process:

In the first step, the abstract protection requirement of the data to be processed is determined on the basis of the data type.

In the second step, the protection requirement must be checked to see if it increases based on the specific data processing circumstances.

In the third step, the protection requirement must be checked to see if it decreases based on specific circumstances.

Ultimately, the protection requirement for the specific data processing operation is classified within a protection requirement category.

4. Protection specification categories for technical and organisation measures

The aim of the protection category concept is to ensure that appropriate protection specifications are defined for and grouped into each protection requirement category.

It is therefore necessary to describe the protection specifications using abstract characteristics in order to fulfil the requirements using various technical and organisation measures.

In setting up a service such as a cloud service, the service provider can select the measures it has to implement with reference to the various protection specification categories. As part of the service certification, an inspection is carried out to verify if the measures would fulfil the requirements of a particular protection specification category. The certification is issued for a particular protection specification and therefore states that the requirements of a particular protection specification category have been met.

This applies in general to all technical and organisational measures. However, differentiation by protection specification categories is not necessary for each and every legal requirement that outsourced data processing has to fulfil. For example, the obligation on the service provider to adhere to the instructions of the user is a legal requirement that is independent of the protection requirement. No differentiation according to protection requirements applies in this regard. The same can be said for the legal requirements that apply to the contract on outsourced data processing.

The requirements to be fulfilled by the technical and organisational measures cannot be assigned by means of a catalogue. For example, it is not possible to simply assign the protection requirement to a particular protection specification category by means of a general password. This is because the use of passwords meets highly varying security requirements, depending on the particular setup and circumstances. With this in mind, there is a considerable need for interpretation of the requirements, taking into account all circumstances attached to the particular setup of the service. This evaluation takes place during the certification as part of the inspection. The inspection and certification must therefore be carried out by qualified certification bodies or inspectors.

A protection category concept alone is not sufficient to ensure a standardised system of inspection and certification throughout the European internal market, as envisaged in the concept drafted by the “Cloud Computing Legal Framework Working Group”. Instead the priority is to formulate, on the basis of legal requirements, a uniform catalogue of requirements that provides for the greatest possible degree of differentiation.

5. Number of protection categories

When establishing protection categories, it is vital to stipulate how many protection categories are to be defined.

Several aspects are significant in this regard.

Define the lowest number of protection categories as possible

The assignment of an individual protection requirement or technical security measure to a protection category must be as simple and unambiguous as possible in order to make the data protection certification manageable for service providers and users. Therefore, the minimum number of protection category should be established.

Define the highest number of protection categories necessary for meaningful differentiation

A minimum level of differentiation is necessary for both service providers and users so that efficient services can be provided. If the differentiation is insufficient, there is a risk that disproportionately high demands will be placed on the technical and organisational security measures. As a result, costs will then be incurred that are not warranted given the actual protection requirement.

Hence there is a need to establish as many different protection categories as are necessary to accommodate differing levels of protection requirement and specifications through various measures with varying costs that can be classified in different protection categories.

Guideline: Differentiation in protection categories according to significantly different demands

To establish protection categories that offer simple and unambiguous assignment of an individual protection requirement to a protection requirement category and also provide sufficient differentiation between services, the number of protection categories must be chosen in such a way that clearly diverging technical and organisational measures with different costs can be assigned to different protection categories.

Concept: 3 and 2 protection categories

The demands mentioned here can be met by a concept that distinguishes between "three plus two" protection categories.

Three protection categories are used as the basis for differentiation; protection requirements (protection requirement categories) and protection specifications (protection specification categories) are described for each of the three protection categories.

The differentiation is based on the assumption that sufficiently clearly different specifications can be defined for three protection categories and that greater differentiation can lead to severe difficulties in the unique assignment of measures to a protection specification category. The distinction between three protection categories appears as the minimum level of differentiation. If there are fewer protection categories, i.e. just two, there is a risk that, in very many cases, demands that considerably exceed the individual protection requirement will need to be met, thus resulting in unnecessary costs.

Two additional protection categories/protection requirement categories are defined for the three protection categories. These additional categories have more of a demarcation and help function. In one protection category, which is called protection category 0 in this protection category concept, the absence of a protection requirement under data protection legislation characterises data that is not personal data and therefore not subject to data protection law.

On the opposite side of the spectrum, a protection category for data processing operations is established, whose protection requirement cannot be described in a protection category and is therefore also not available for a higher-level certification. This affects data processing operations with an extremely high protection requirement and individually highly diverging circumstances. This situation is known as a "three plus (3 +)" protection category in this concept.

In this case, a risk analysis is carried out by the responsible party wishing to have data processed by a provider as part of an outsourced data processing agreement. Based on this analysis, the party responsible determines, in particular, the requirements to be met by the technical and organisational measures of the service provider and ensures that the service provider meets the demands.

In the case of protection categories 0 and 3+, the description of the protection categories is restricted to the protection requirement categories because, in this respect, no protection specifications or no supra-individual protection specifications under data protection law can be determined.

6. Applying the protection category concept to the certification and use of services

Applying the protection category concept to the certification and use of a certified service leads to a differentiated distribution of tasks between the provider, the user of the service and the certification body.

The provider guarantees a specific protection requirement category when processing the data and applies for certification for the corresponding protection specification category.

Based on an inspection conducted as part of the certification procedure, using the designated technical and organisational measures, the certification body assigns the service to a certain protection category. The suitability of the service for a specific protection specification category is expressed in the certificate.

The user of the service assigns the protection requirement of its specific data processing operation to a certain protection requirement category. In doing so, the user performs the described assignment in the three steps mentioned above. On this basis, the user can choose a service that is certified for the relevant protection category.

7. The protection categories in the Trusted Cloud data protection profile for cloud services

The Trusted Cloud data protection profile for cloud services (TCDP) is based on the protection category concept described here. Where necessary, distinct specifications for the protection categories are described accordingly for the standards and implementation recommendations.

III. The protection categories

The protection requirement categories are defined and explained using examples on the following pages. (1.) Thereafter, the assignment of the protection requirement of a data processing operation to a protection requirement category is outlined in a three-stage procedure (2.) In this procedure, the abstract protection requirement categories are initially defined according to the relevant data type (2.1) and thereafter the factors leading to an upgrading (2.2) or downgrading of the protection requirement (2.3) are outlined. The protection specification categories are then described (3.).

1. Protection requirement categories

1.1 Protection requirement category 0

Data processing operations (i.e. the service required from the cloud service) that do not contain, generate, support or facilitate any information at all or any information in need of protection about the personal circumstances of individuals.

Example:

The cloud service user wants to save only weather data or personal data that has been shared by the affected party for any type of collection, processing or use.

Note:

The release of personal data does not preclude that collection, processing or usage bans exist for certain bodies with regard to the released data.

1.2 Protection requirement category 1

Data processing operations (i.e. the service required from the cloud service) that, as a result of the data included and the specific collection, processing or use of this data, contain, generate, support or facilitate information about the personal circumstances of the affected party. The unauthorised use of this data can be easily prevented or intercepted by the affected party's actions.

Example:

The cloud service user needs to save and process address data for its contract partner (for form letters). Because of the nature of the data (names, addresses) and processing operation involved (saving, processing for form letters), this data processing operation (saving) contains information about the personal circumstances of the contract partners.

1.3 Protection requirement category 2

Data processing operations (i.e. the service required from the cloud service) that, based on the data used or the specific collection, processing or use of this data, contain, support or lead to information about the identity or circumstances of a person (affected party). The unauthorised processing or use of this data can disadvantage the affected party (impairment of their legal rights).

Example:

The cloud service user needs to save and process banking and credit card data for clients. Because of the nature of the data and the processing operation, this data processing operation contains information about the financial circumstances of the contract partners.

1.4 Protection requirement category 3

Data processing operations (i.e. the service required from the cloud service) that, based on the data used or the specific collection, processing or use of this data, contain, support or lead to important information about the identity or circumstances of a person (affected party). The unauthorised collection, processing or use of this data can seriously disadvantage the affected party.

Example:

The cloud service user needs to save the diagnoses of cancer patients.

1.5 Protection requirement category 3 plus

Data processing operations (i.e. the service required from the cloud service) that, based on the data used or the specific processing or use of this data, contain, support or lead to important information about the identity or circumstances of a person (affected party). The unauthorised collection, processing or use of this data can lead to a definite risk of critically impairing the life, health or freedom of the affected party.

Example:

The cloud service user wants to save data concerning trusted agents of the intelligence services. An unauthorised release of such data could endanger the health and lives of the affected parties.

2. Determining the protection requirement of a data processing operation

The protection requirement is determined in a three-stage procedure:

In the first step, the abstract protection requirement of the data to be processed is determined on the basis of the data type.

In the second step, the protection requirement must be checked to see if it increases based on the specific usage.

In the third step, the protection requirement must be checked to see if it decreases based on the specific circumstances.

Ultimately, the protection requirement for the specific data processing operation is categorised according to the above-mentioned protection requirement categories.

2.2 Protection requirement categories based on data type (abstract protection requirement - step 1) 2.2.1 Data without protection requirement (data protection category 0)

Non-personal data, including effectively anonymised data as well as data that has been effectively "shared" by the affected party, in other words published for unrestricted collection, processing or use.

Examples:

- Synthetically generated test data ("John Smith")
- Weather data
- Effectively anonymised data
- Effectively shared data

2.2.2 Data types with normal protection requirement (protection requirement category 1)

Personal data (individual details about the personal or material circumstances of the affected party, Section 3(1) Federal Data Protection Act).

Examples:

- Name, address (excluding context), provided it is not protection requirement 2 or 3
- Nationality (excluding context), provided it is not protection requirement 2 or 3
- Telephone number of an individual, provided it is not protection requirement 2 or 3

2.2.3 Data types with high protection requirement (protection requirement category 2)

Data types contain specific information about the identity and/or circumstances of the affected party. The unauthorised collection, processing or use of such data can lead to unlawful interference in the right to self-determination about personal information.

Examples:

- Name, address of a contract partner (provided it is not protection requirement 3 or 3+)
- Date of birth
- Context surrounding a contract partner (e.g. subject of an agreed service)
- Religious denomination
- Simple feedback of rather low significance (e.g. a yes/no decision regarding a categorisation in a mobile phone plan, etc.)
- Access data to a service (provided it is not protection requirement 3 or 3+).
- Communication contents relating to an individual (e.g. email content data, letter, phone call) (provided it is not protection requirement 3 or 3+).
- (Precise) place of residence of an individual (provided it is not protection requirement 3 or 3+)
- Financial data relating to an individual (e.g. bank balance, credit card number, individual payment)
- Telecommunications traffic data

Note: Contents of communication

The contents of any communication, in particular any type of written or verbal records, can have very different protection requirements, from low to very high. Specification of the protection requirement requires a subjective assessment, which is incumbent on the person responsible for the communication. The fact that an individual utterance is classified by the person voicing it as requiring protection or is objectively deemed (by a third party) to be particularly in need of protection should, however, not lead to a situation where every communication is deemed to be particularly in need of protection. In particular, the cloud service user does not necessarily need to know the subjective protection requirement of the person responsible for the particular communication.

Example: A cloud service user subscribes to a collaboration service with data storage, video conferencing and email functionality. The cloud service user therefore should be able to assume that protection requirement category 2 is needed, provided that no other specific information exists about the protection requirement (example: a conference service is booked for a conference between a solicitor and their client, in this case, the protection category is 3).

2.2.4 Data types with a very high protection requirement (protection requirement category 3)

Data types contain important information about the identity and/or circumstances of the person. The unauthorised collection, processing or use of such data can lead to a serious unlawful interference in the right to self-determination about personal information.

Note:

Bulk data, especially interlinked data (e.g. a personality profile), from which new information content can be derived, is also considered a data type in this respect.

Examples:

- Data that is subject to professional confidentiality (e.g. patient data)
- Data regarding a person's previous convictions and judicial circumstances (e.g. judicial inquiries)
- Behavioural profiles, e.g. mobility profile, purchasing behaviour profile, containing important information about the identity of the affected party

2.2.5 Data types with an extremely high protection requirement (protection requirement category 3 plus)

Data types contain important information about the identity and/or circumstances of the person. The unauthorised collection, processing or use of this data can lead to a definite risk of critically impairing the life, health or freedom of the affected party.

Example:

Data concerning trusted agents of the intelligence services

2.3 Upgrading (step 2)

Principle:

The protection requirement of a data processing operation can be upgraded due to various circumstances if a risk of a greater impairment of the personal rights of the affected party arises. The protection requirement upgraded in this way can, depending on the extent of the protection requirement achieved, lead to classification in a higher protection requirement category. The following factors in particular can lead to upgrading of the protection requirement:

- The context in which the data are used
- The degree to which the data are interlinked
- Quantity of data

2.3.1 Context in which the data are used

The context in which the data are used can lead to a higher protection requirement, insofar as it provides a (significantly) greater amount of information about the identity of the affected party.

Example:

The use of the name in a (general) telephone book does not generally constitute an increased level of information; the use of the name in a doctor's patient list certainly does, and in some circumstances it even significantly increases the level of information. The following are examples of how the context in which data are used upgrades the protection requirements.

- Data type: Name, address
- Context in which the data are used: Certificate of good conduct; criminal file; photo database of perpetrators; employee screening; HR file

2.3.2 Degree to which data are interlinked

The extent to which the data are interlinked, i.e. the possibility of linking data with other data and as a result acquiring new information, can lead to a higher protection requirement, provided that the interlinking results in the data having a (considerably) greater information value regarding the identity of the affected party. This also applies when one item of data is linked with other data of the same or a lower protection requirement category.

Example:

The linking of data about the purchase of products (protection requirement category 2), and if applicable additional data of the same or another type, such as place of residence (protection requirement category 2), can certainly lead to an accurate behavioural profile depending on the number of individual items of data. Such a behavioural profile can be classified as protection requirement category 3.

Examples of the kind of data interlinking that upgrades the protection requirement:

- Location data that can be consolidated specifically in one mobility profile (the consolidation is possible and logical in the specific situation).

2.3.3 Quantity of data:

Given the sheer quantity of data available, there may be an increased interest in the unauthorised processing and use of data exists with the result that there is a greater risk of unauthorised processing and use also in relation to each individual item of data.

Example:

Saving a large quantity of credit card data at one location can make this data a worthwhile target of attack for criminals which means that the probability of an attack increases. The threat therefore increases for all credit card data stored there.

The following are examples of the centralisation of data which increases the protection requirement.

- Collection of large quantities of bank and credit card data

2.4 Downgrading (step 3)

The protection requirement of one data protection operation can be downgraded due to various circumstances, provided that the risk of an attack is reduced or the information value of the data is decreased on the basis of these circumstances or certain measures that have been taken. The protection requirement downgraded in this way can, depending on the extent of the protection requirement achieved, lead to classification in a lower protection requirement category.

Example: With the (effective) pseudonymisation of data, the information value for anyone who does not know the assignment rule, is reduced considerably.

The following circumstances in particular can lead to downgrading:

- Information content and context in which it is used
- Encryption of data
- Pseudonymisation of data (Section 3(6a) Federal Data Protection Act)
- Release of data

Note:

The encryption and pseudonymisation of data are measures used to protect personal data.

Both encryption and pseudonymisation therefore have a dual significance: From the point of view of the cloud provider, they influence the protection requirement of data. Data thus has a lower protection requirement when it is provided to the cloud provider in encrypted form. Nevertheless, encryption is one of the measures that can be used by the cloud provider to protect data from being accessed by unauthorised parties.

2.4.1 Information content and context in which it is used

Due to its information content and the context in which it is used, data can be less informative about the identity of the affected party and this party's circumstances than the abstract classification of the data type would suggest.

Example: The arrangement of a patient's appointment with their family doctor must be classified as health data. However, the appointment information in itself is not informative enough to warrant protection requirement category 3 and corresponds instead to other location data, as it may involve a routine visit from which no additional information about the person's circumstances can be derived.

2.4.2 Encrypting data

The encryption of data involves changing personal data in such a way that, unless it is decoded, there is no way of knowing the content of the data or it can only be ascertained with a disproportionately high amount of effort.

2.4.3 Release of data

Data that needs to be protected can be shared by the affected party for collection, processing and use. In this case, the affected party has downgraded the protection requirement. The data may even be freely available and the protection requirement can be downgraded to protection requirement category 0.

Example: A patient publishes his or her medical record on the internet to draw attention to a particular illness and facilitate research.

3. Protection specification categories

The protection specification categories describe the specifications that must be fulfilled for data processing operations in the corresponding protection requirement category. A protection specification category of 0 does not need to be described: in this respect no specifications exist in terms of data protection law. No description will be provided for protection specification category 3 plus, as it is difficult to describe the specifications in general terms as they are usually very specific to individual cases. In this respect, the statutory – case-by-case related – standard applies.

3.2.

Protection specification category 1

The service provider must guarantee, through risk-appropriate technical and organisational measures, that the data will be protected from unauthorised processing or use.

The measures must be adequate to generally rule out such operations based on technical or organisational errors, including operating errors or negligent handling by third parties (cloud service users, other third parties). Minimum protection must be provided to impede deliberate interference.

3.3.

Protection specification category 2

The service provider must guarantee, through risk-appropriate technical and organisational measures, that the data will be protected from unauthorised processing or use.

The measures must be adequate to generally rule out such operations based on technical or organisational errors, including operating errors or negligent handling by third parties (cloud service users, other third parties). Protection against deliberate interference must be provided, which rules out with sufficient certainty the expected interference. This includes in particular sufficient protection against known attack scenarios as well as measures by means of which interference can generally (retrospectively) be identified.

3.4.

Protection specification category 3

The service provider must guarantee, through state-of-the-art and risk-appropriate technical and organisational measures, that the data will be protected from unauthorised processing or use.

The state-of-the-art measures must be adequate to rule out with sufficient certainty such operations based on technical or organisational errors, including operating errors or negligent or deliberate action on the part of the cloud service provider and its employees or third parties (other cloud service users, other third parties). This includes in particular sufficient protection against known attack scenarios and procedures to identify abuses.

Authors

Dr. Thorsten B. Behling, WTS Legal Rechtsanwaltsgesellschaft mbH

Oliver Berthold, Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit)

Prof. Dr. Georg Borges, Trusted Cloud Competence Centre

Dirk Bungard, Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)

Mathias Cellarius, SAP SE

Susanne Dehmel, BITKOM e. V.

Thomas Doms, TÜV Trust IT GmbH

Dr. Alexander Duisberg, Bird & Bird LLP

Dagmar Hartge, Brandenburg State Commissioner for Data Protection and Access to Information (Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg)

Dr. Hubert Jäger, Uniscon universal identity control GmbH

Thomas Kranig, Data Protection Supervisory Authority of Bavaria (Bayerisches Landesamt für Datenschutzaufsicht)

Johannes Landvogt, Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)

Dirk Piesker, Deutsche Telekom AG

Christoph Rechsteiner, SAP SE

Frederick Richter, Federal Foundation for Data Protection (Stiftung Datenschutz)

Gabriel Schulz, Mecklenburg-Western Pomerania State Commissioner for Data Protection and Freedom of Information (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern)

Antonius Sommer, TÜV Informationstechnik GmbH

Dr. Mathias Weber, BITKOM e. V.

Andreas Weiss, Eurocloud Deutschland_eco e. V.

Monika Wojtowicz, TÜV Informationstechnik GmbH

Ursula Zabel, Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit)

Publishing details

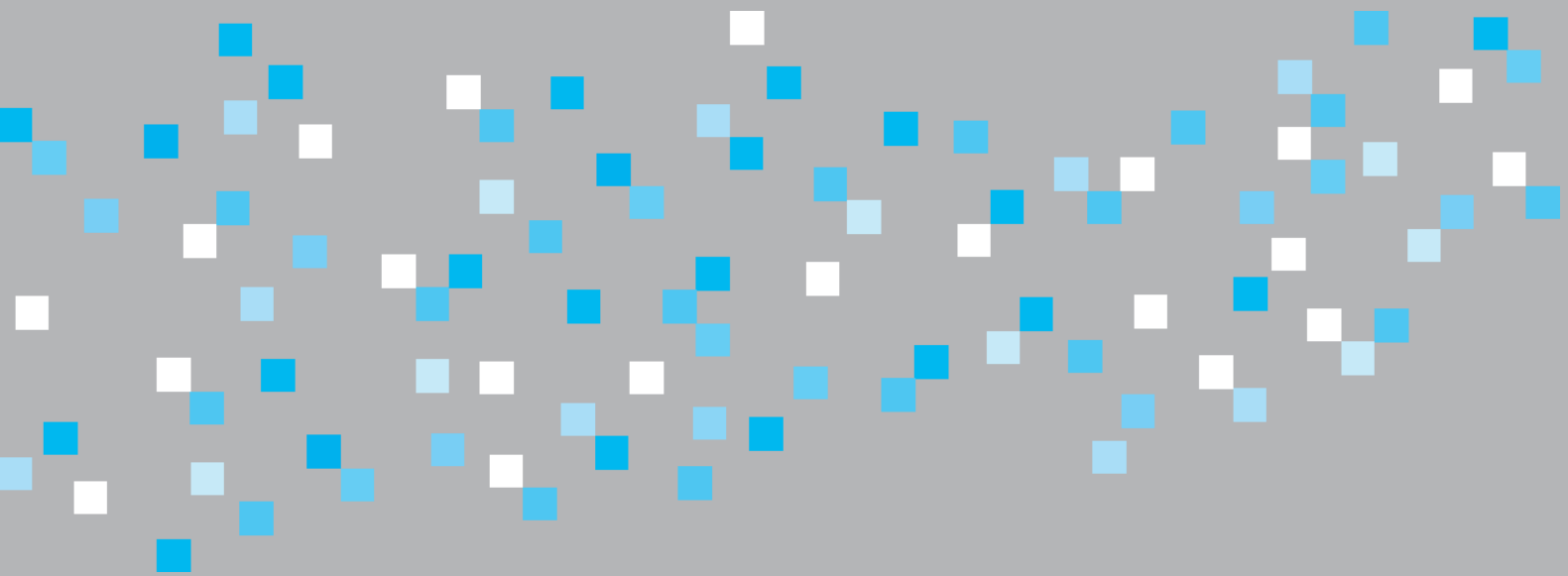
Published by
Trusted Cloud Competence Centre
Working group: Legal Framework for Cloud Computing
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

On behalf of the Federal Ministry for Economic Affairs and Energy (BMWi)

Design
A&B One Kommunikationsagentur, Berlin

Printed by
DCM Druck Center Meckenheim

As at: March 2014



www.trusted-cloud.de