

Trusted Cloud Competence Centre

**Position Paper –
Basic Principles of
a Certification
Procedure for
Cloud Services**

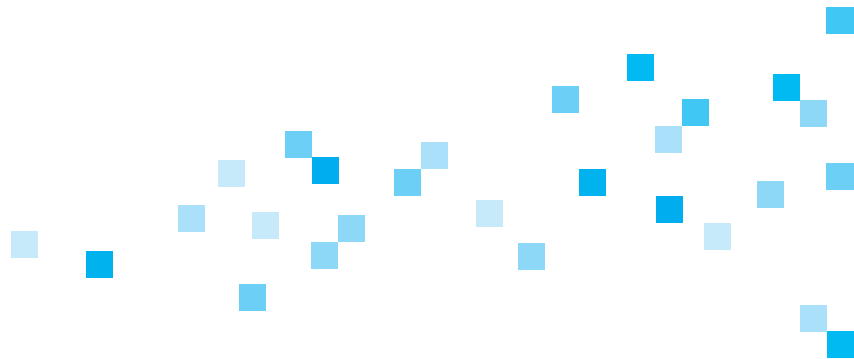
Nr. **12**



Cloud Computing Legal Framework 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.



Contents

1	The certification of cloud services	6
	The challenge — efficient data protection in cloud computing	6
	The solution — certification of cloud services by independent third parties	7
2	The certificate	8
	The certificate's content and declaration	8
	The certificate's legal effect	9
	The certificate's scope and period of validity	10
3	Awarding of certificates	11
	Certification procedure	11
	Inspection requirements and inspection intensity	11
	Costs of the certification procedure	12
4	Inspection bodies and certification bodies	13
	Differentiating between an inspection body and a certification body	13
	Requirements for certification bodies and inspection bodies	14
	Accreditation procedure	15
5	Revoking certification, liability and legal recourse	16
	Revoking certificates	16
	Liability in the event of incorrect certification	17
	Legal recourse	19
6	Conclusion	20
	Authors	22

1 — The certification of cloud services

In its proposition paper entitled “Cloud Computing Solutions in the Field of Data Protection Law”, published in September 2012, the “Cloud Computing Legal Framework” Working Group within the Trusted Cloud Competence Centre of the Federal Ministry for Economic Affairs and Energy (BMWi) described a concept for the certification of cloud services in accordance with data protection law.

The core elements of this concept are being developed in detail in the pilot project “Data Protection Certification for Cloud Services”, which was launched in November 2013 and is operated by the Trusted Cloud Competence Centre together with project partners on behalf of the Federal Ministry for Economic Affairs and Energy. A key component of this work involves the description of a suitable certification procedure.

→ The challenge — efficient data protection in cloud computing

Cloud computing services normally process data on behalf of the cloud service user. If personal data is processed, this is viewed as outsourced data processing under data protection legislation, specifically Section 11 of the Federal Data Protection Act (BDSG), according to which the cloud service user acts as the client or principal, while the cloud service provider acts as the processor or agent. As a result, the cloud service user is, under Section 11(1) of the Federal Data Protection Act, responsible for ensuring compliance with data protection legislation. Current German and European data protection legislation and the draft EU General Data Protection Regulation demand that the client must verify that the processor is also compliant with legal data protection requirements.

If a company uses cloud computing services to process personal data, the company must ensure that data processing by the cloud service provider satisfies the provisions of data protection legislation. For this purpose, the technical and organisational measures put in place by the cloud service provider must be inspected. According to Section 11(2) sentence 4 of the Federal Data Protection Act, the cloud service user, as the client, must ensure that the technical and organisational measures put in place by the cloud service provider are compliant both before the commencement of data processing and at regular intervals thereafter, and the result of these inspections are to be documented in accordance with Section 11(2) sentence 5. If the cloud service user fails, either intentionally or through negligence, to ensure that the technical and organisational measures put in place by the processor are legally compliant before the start of data processing, the cloud service user is, according to Section 43(1) sentence 2b of the Federal Data Protection Act, guilty of an administrative offence, which is punishable by a fine of up to 50,000 euros under Section 43(3) of the Federal Data Protection Act.

However, it would be excessively costly for each individual cloud service user to inspect the cloud service provider’s technical and organisational measures. Small companies that use cloud services would not, in any case, have sufficient resources to conduct such inspections themselves. A further problem with the client’s obligation to inspect the service provider is that users will frequently make use of many different cloud systems, while one cloud system may be accessed by many different users. This means that each

cloud service user would have to inspect a range of services and that each individual service would, in turn, need to be inspected by many different users.

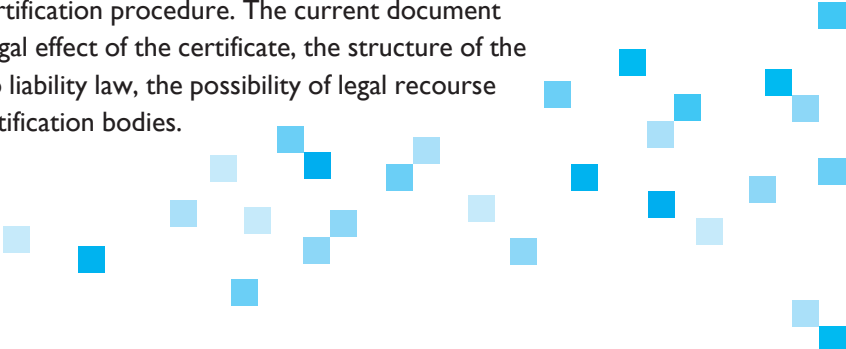
The solution —

→certification of cloud services by independent third parties

This structural problem can be solved by bundling inspections. This would involve establishing a suitable certification procedure covering all obligations that a processor of outsourced data in cloud computing (i.e. a cloud service provider) is required to meet under data protection legislation. This procedure would be used in particular to ensure that the technical and organisational measures put in place by the cloud service provider are inspected by a suitably qualified independent certification body according to accepted standard criteria (see Section IV.2). If all requirements under data protection law are fulfilled, a certificate is issued to confirm this. The result of the inspection would be of benefit to all users of the inspected cloud service. In addition to guaranteeing a high level of data protection, this type of certification would also establish an efficient basis for the use of cloud services.

This type of bundling of inspections is, in principle, already permitted under the current legislation. The inspection required under Section 11(2) sentence 4 of the Federal Data Protection Act does not have to be conducted by the client in person, and may also be performed by an independent third party. This third party can also conduct the inspection for several clients at the same time, provided that the inspection requirements of each of the individual clients are met. However, significant legal uncertainty exists in relation to the requirements that can be specified for a test or certificate of this kind, as well as in relation to the legal consequences associated with these. At present, there is no legal regulation of certification at federal level.

It was with this solution in mind that the Federal Ministry for Economic Affairs and Energy launched the pilot project “Data Protection Certification for Cloud Computing” in November 2013. The project forms part of the Ministry’s “Trusted Cloud” technology programme, which develops and tests innovative, secure and legally compliant cloud computing solutions. This pilot project takes account of the current provisions of the Federal Data Protection Act, while also discussing issues that are of relevance for the future EU General Data Protection Regulation. One objective of the pilot project is to describe the cornerstones of a suitable certification procedure. The current document focuses in particular on the content and legal effect of the certificate, the structure of the certification procedure, aspects relating to liability law, the possibility of legal recourse and the requirements to be fulfilled by certification bodies.



2 — The certificate

→ The certificate's content and declaration

Within the concept developed by the “Cloud Computing Legal Framework” Working Group, the certificate is a declaration of knowledge issued by the certification body, which states that the inspected service complies with the requirements of data protection legislation. The inspection conducted as part of the certification procedure focuses in particular on the compliance of the technical and organisational measures put in place by the cloud service provider in order to meet the requirements of data protection legislation. As a result of certification, an attestation, i.e. a certificate of compliance with the relevant norms under data protection legislation is issued. In this context, the synonymous term “compliance certificate” may also be used. This paper uses the term “data protection certificate”.

Certification can, in this sense, be viewed as distinct from processes that end with the granting of a quality mark. This is because, in the case of a quality approval process, not only the current legal norms but also additional or alternative assessments based on data protection legislation can be taken into account alongside the current legal standards that serve as the key inspection criteria. Certification also differs from processes where one or more aspects of data protection legislation are taken into account but not all legal requirements (i.e. requirements under data protection law) are inspected.

Since the main focus of the inspection is on determining whether the cloud service provider has implemented the necessary technical and organisational measures, the inspection is dependent on an evaluation to assess which measures are essential. According to Section 9 sentence 2 of the Federal Data Protection Act, measures are only considered necessary if the effort they involve is commensurate with the objective they are designed to achieve in terms of protection. The Appendix to Section 9 of the Federal Data Protection Act, which lists examples of necessary control measures, specifies which type of personal data is to be protected. For example, proportionately stricter requirements may need to be met, depending on the protection required for the data that is to be processed and the data processing procedure as a whole. If, as part of the cloud service, personal data as defined by Section 3(9) of the Federal Data Protection Act (for example, personal health data), the technical and organisational measures must take account of the heightened security requirements. Therefore, cloud services that provide for adequate security measures for the processing of “regular” personal data, such as customer master data, are unsuitable for the processing of personal health data. In this context, the certificate must also specify the data protection category for which the cloud service is suitable. This also indicates to the cloud service user whether a cloud service on offer meets the unique requirements of the user's data processing scenario.²

²
www.trusted-cloud.de.

→ The certificate's legal effect

The certificate represents a declaration of knowledge by the certification body, stating that the inspected cloud service fulfils the requirements under data protection legislation, and that the required technical and organisational measures are compliant. However, this is not a statement of the legal effect of such a certificate.

The implementation of a certification procedure by a cloud service provider is, firstly, an expression of conscious and deliberate self-regulation.

Certificates provide market incentives by creating transparency and trust and, as a result, offer competitive advantages for the services inspected. Certificates provide an efficient way for users to inform themselves and to compare offerings.

In addition, the certification of cloud service providers makes it easier for the user to be certain that the technical and organisational measures put in place by the cloud service provider are compliant, as required under Section 11(2) sentence 4 of the Federal Data Protection Act (see Section 1.2). However, due to a lack of explicit regulation, a considerable degree of legal uncertainty exists with respect to the conditions under which the use of a certified service exempts the cloud service user from the legal requirement to verify that the relevant requirements are being fulfilled. To establish the legal certainty required, the future EU General Data Protection Regulation should include a provision stipulating that a company can fulfil its obligation of ensuring the compliance of a cloud service by using a cloud service that has been certified in accordance with legal provisions. Users could then place their trust in the certificate and use the cloud service in a way that complies with data protection legislation without themselves having to inspect the cloud service.

Statutory provisions should also dictate that the cloud service user must actually see the certificate as a means of verifying that the service is suitable for the intended data processing. In other words, the mere existence of a certificate for a service should not eliminate the user's own supervisory duty. Similarly, according to the current legislation, a penalty cannot be avoided on the basis of the objective existence of technical and organisational measures. On the contrary, the party responsible must verify that these measures are legally compliant and the Federal Data Protection Act Section 11(2) sentence 5 requires that the result of this verification be documented. Another important reason for making it mandatory for users to inspect the certificate is that this provides a means of determining whether the cloud service is suitable for the intended data processing purpose, in particular with regard to the requirements for protecting the data to be processed. A legal documentation requirement, similar to the requirement that already exists, would demand that the cloud service user furnishes evidence that the certificate had been viewed and inspected. Against this backdrop, the EU General Data Protection Regulation should include a provision stipulating that a cloud service user can fulfil the obligation to verify that the technical and organisational prerequisites are met by inspecting the cloud service provider's certificate and by then determining and documenting the suitability of the service for the intended data processing. Once these obligations have been met, a fine cannot be imposed on the cloud service user, even if the cloud service user has not personally verified that the provider's technical and organisational measures are legally compliant.

The certificate also has legal significance should follow-up issues arise, in particular if the cloud service user is held responsible for a violation of data protection law. The existence of a certificate does not hinder the data protection authorities in the fulfilment of their advisory and monitoring tasks, and does not present an obstacle to the issuing of orders if the regulatory authority is not satisfied that the legal obligations under data protection legislation have been met despite the existence of a certificate. However, insofar as the data protection authority may consider issuing a fine based on the finding of an administrative offence, the certificate must be taken into account in investigating a culpable breach of legal obligations. Since the cloud service user has fulfilled its fundamental legal obligation by inspecting the certificate, there is normally no culpable breach of obligations. Accordingly, the issuing of a fine is normally only considered if the cloud service user can be accused of another breach of duty, for example, if the user had previous knowledge of the data protection violation. The same applies to civil proceedings, for example, if the party concerned brings a claim for damages on the basis of unauthorised data processing.

European legislators could also put provisions in place to regulate whether and under which conditions the existence of a certificate can be considered an adequate basis for secure transmission of data to a third country, and thus as providing an alternative to the Safe Harbour agreement or to the conclusion of standard EU contracts. According to the planned new legislation, a certificate could also be afforded additional legal effects (e.g. certified services being favoured in contract award procedures).

As mentioned earlier, the certificate represents a declaration of knowledge by the body that issues it. More detailed specifications in the future EU General Data Protection Regulation in particular, or the delegated acts adopted on the basis of this Regulation will determine whether this is to be a declaration under private law or an administrative act (by an authority acting as a certification body or by a private certification body entrusted with this task). This should have no impact on the legal effect of the certificate.

→ **The certificate's scope and period of validity**

Certifications of cloud services primarily concern technical and organisational measures that, because of technical progress, are only valid for a limited period. Provision should therefore be made for the certificates to be valid for a maximum of three years, after which re-certification is required. The need for interim inspections should also be regulated. Provision should be made for a simplified inspection process for the purpose of re-certification following expiry of the validity period. This simplified process should be based on changes in the factual or legal situation that have occurred since the initial certification.

The certification should be valid throughout the entire territory that falls within the scope of the EU General Data Protection Regulation in order to establish legal certainty for cloud service providers and cloud service users across the entire internal market and to avoid conflicting decisions in different member states. This would also be in keeping with the objective of the EU General Data Protection Regulation to guarantee a standardised level of data protection across the EU, while also eliminating discrepancies that could hamper the free movement of data within the internal market

3 — Awarding of certificates

→ Certification procedure

The certification procedure is initiated by means of an application by the cloud service provider, seeking certification for the purpose of self-regulation or in order to achieve competitive advantages for the cloud service. In the EU General Data Protection Regulation, the completion of a certification procedure should be envisaged as a voluntary undertaking rather than as an obligation. Following the submission of an application by the cloud service provider or after a contract for the implementation of a certification procedure has been concluded, the inspection body responsible inspects the service based on a set of predefined inspection requirements. Based on the inspection report by the inspection body, i.e. following a review of the documentation on file, the certification body then decides whether the requirements of data protection law have been fulfilled, and therefore whether a certificate is to be granted or denied. The certificate must be published by the certification body itself or by another body determined by law. The date of issue and the date on which the validity of the certificate expires must be specified on the certificate.

→ Inspection requirements and inspection intensity

The inspection procedure is based on defined inspection requirements or inspection criteria, in other words, specific requirements that must be fulfilled before a certificate can be awarded. It is with this in mind that a data protection inspection catalogue for cloud services, the “Trusted Cloud Data Protection Profile for Cloud Services” (TCDP), is currently being developed as part of the “Data Protection Certification for Cloud Computing” pilot project. The TCDP will specify the legal requirements for cloud services based on the Federal Data Protection Act, and will thus also serve as a template for the requirements arising from the future EU General Data Protection Regulation.

Standardized inspection requirements for the awarding of certificates should be defined by law for the entire European internal market. While a definition of the inspection requirements in the EU General Data Protection Regulation itself would enable standardized legislative control, it would however overload the text of the Regulation and make it too inflexible. Therefore, the inspection requirements should be defined in a process that involves the participation of regulatory authorities as well as representatives of the providers and users of outsourced data processing services.

The required technical and organisational measures are essentially determined on a case-by-case basis, and their definition will necessitate a weighing of the need for protection against the effort involved in achieving it (see Section 9 of the Federal Data Protection Act). Therefore, it is not possible to define in general terms the measures required in each individual case. However, this does not exclude the possibility of having standardised certificates. It must first be considered that the majority of requirements to be fulfilled by the technical and organisational measures put in place by cloud service providers are identical for a large number of data processing operations. This means that similar requirements can be formulated for most areas of application. To the extent that

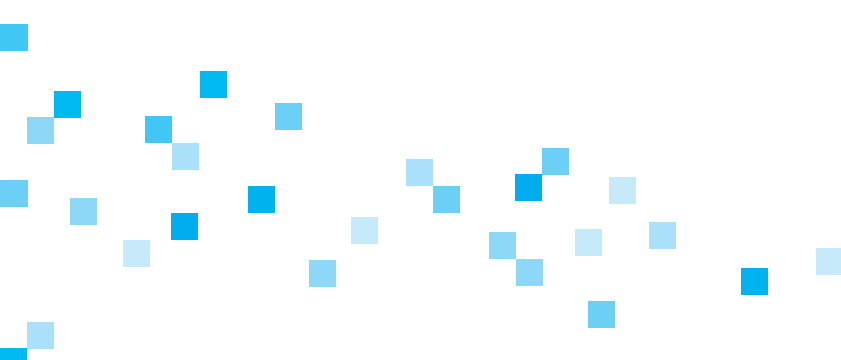
the client must fulfil special statutory requirements, in particular because of the type of data involved (e.g. health data), case groups can be created and these can be taken into account as part of certification, and can be indicated on the certificate by specifying a corresponding protection category. The same applies if the risk profile of the data processing is changed due to special technical protection measures.

In terms of the inspection intensity underlying the certification procedure, it is crucial for transparency to be created for the cloud service provider and, in particular, for the cloud service user. For example, when regulating the certification procedure, it is necessary to specify, as clearly and precisely as possible, how the inspection is to proceed during certification and the degree of detail to be included in inspections of the individual requirements. For the certification of a cloud service, it is often necessary to conduct an on-site inspection of the compliance of the technical and organisational measures that have been implemented by the cloud service provider.

→ Costs of the certification procedure

Given that the costs of a certification procedure largely depend on the inspection requirements (which are as yet undefined) and the inspection depth (similarly not yet defined in law), the pilot project cannot provide a precise indication of the expected costs associated with a certification procedure.

It is not considered necessary to introduce statutory regulation of these costs. Instead, they should be determined by market forces, in as far as the service is provided within the private sector. While the fees collected should allow certification bodies to cover the costs of operation and to generate profits, they should still remain affordable for cloud service providers and, in particular, not act as a deterrent to applying for certification. Otherwise, the impact on the desired propagation of certificates in the market would be significant.



4 — Inspection bodies and certification bodies

→ Differentiating between an inspection body and a certification body

Data protection certification comprises two essential steps. First, the cloud service is inspected on the basis of the applicable inspection requirements, which are to be documented in an inspection report (see above). Second, it is decided, on the basis of the documented inspection, whether the desired certificate is to be awarded, awarded subject to restrictions, or denied. The body that conducts the inspection is referred to as the inspection body, while the body that makes a decision as to whether to award certification is referred to as the certification body. It is essential to distinguish between an inspection body and a certification body from a functional perspective.

A functional division of the inspection and certification roles does not necessarily presuppose a separation of the inspection body and certification body from a legal and organisational perspective. However, there are strong arguments in favour of also creating an organisational distinction between the inspection body and the certification body and, accordingly, assigning each of these bodies a separate set of tasks. There are also good reasons for at least making a legal separation possible. This would allow specialised units to evolve, with a specific focus on either inspection or certification. Many certification procedures are organised this way in the area of data protection and IT security. The organisational and legal separation of the inspection body from the certification body can therefore be regarded as a proven standard.

A legal separation between inspection body and certification body means that each is to be assigned a separate set of responsibilities. In addition, independent legal relationships arise between the inspection body and cloud service provider on the one hand, and between the certification body and the cloud service provider on the other. This legal relationship may take the form of a private-law contract or an administrative procedure. In any event, the legal relationship between the inspection body and the cloud service provider must be established as a private-law relationship, as has been the practice to date. The legal relationship between the cloud service provider and the certification body can be established as a relationship under private or public law as set out in the paper “Data Protection Certification by Private Bodies”.

According to this configuration, the cloud service provider is the contractual partner of the inspection body and has a legal relationship with the certification body. The cloud service provider can therefore choose which inspection body and which certification body to use. If a market for the inspection and certification of cloud services is to be allowed to develop, this choice should not be restricted.

In this context, the greatest difficulties arise in connection with the relationship that exists between the inspection body and the certification body. Due to the organisational and legal separation between the two, it is not essential for a legal relationship to exist between them for the purpose of certification. Currently, certification bodies often restrict the choice of inspection body as part of their conditions of certification by only allowing certain inspection bodies to be used. This would appear appropriate based on the current

legislation, according to which no legal quality control exists for inspection bodies or inspection. However, this is unlikely to continue to be the case in the context of legally formalised data protection certification. As an alternative, the European legislator could also establish a system whereby the inspection body and the inspection, including the inspection report, must meet certain quality requirements, while the certification body, for its part, must accept an inspection conducted by any inspection body that fulfils these requirements. Finally, it would also be conceivable that a certification body would, despite the existence of legally formalised quality requirements, have the option of imposing its own requirements on inspection bodies or inspection reports. However, this would only be justifiable if cloud service providers were able to choose between a sufficient number of certification bodies. The certification body should, in any case, be able to specify requirements in terms of the language and, where not regulated by law, the form of the inspection report.

→ Requirements for certification bodies and inspection bodies

Regardless of whether the inspection body and certification body form part of the same organisation or are legally independent entities, it is essential to specify in the legislation the requirements that apply to certification and inspection bodies and whether certification is to be the remit of private or public bodies.

The possibility of awarding data protection compliance certificates in accordance with the EU should not be limited to regulatory authorities and should also be open to private bodies. This can only be clarified in the EU General Data Protection Regulation.⁷

With regard to the question of which substantive requirements are to apply to certification bodies, it must be remembered that both cloud service providers and cloud service users will only make use of the certificates offered if they can place their trust in these certificates. This trust depends on the reliability of the statements made by the certification bodies. The qualifications and independence of the certification bodies are essential to ensuring the quality and acceptance of certificates in the market and among regulatory authorities. To lay down these prerequisites in more concrete terms, the legal requirements to be fulfilled by certification bodies must be defined. For example, the qualifications possessed by a certification body should be subject to verification, in particular with regard to expertise, organisation and resources. This applies above all to the personal and professional skills and qualifications of the persons responsible for certification. Furthermore, the certification body must exercise its duties independently. In other words, it must remain, above all, uninfluenced by extraneous factors. To ensure that conflicts of interest and dependent relationships are avoided to the greatest extent possible, the procedure must be as transparent as possible, and the result of the inspection result must be presented in a clear and objective manner.

These proposals apply equally to inspection bodies. Their qualifications and independence must be guaranteed to the same degree in order to protect the validity and acceptance of the certificates. The trustworthiness of the content presented in the inspection report must be guaranteed by virtue of the fact that the certification body decides whether or not to award a certificate on the basis of the inspection result and the fact that the certification body can only verify the credibility of the inspection report

⁷ www.trusted-cloud.de

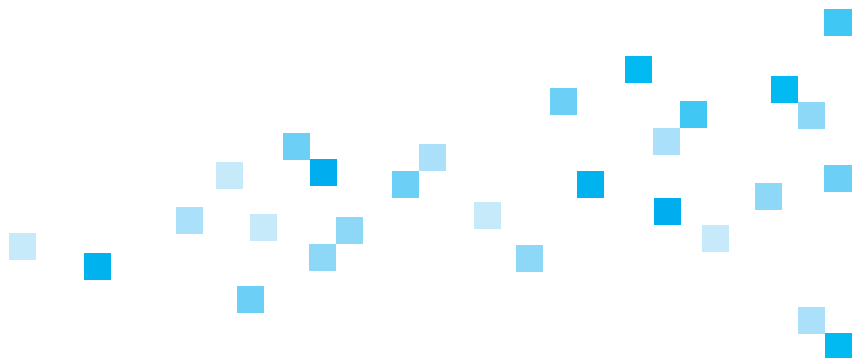
on the basis of the documentation it receives. It is therefore necessary to establish a legal framework for the requirements that apply to the inspection and to the inspection report. This framework should also include a definition of the format of the inspection report (e.g. by providing a template) so that inspection reports can be used throughout the internal market.

→ Accreditation Procedure

An accreditation procedure should be put in place to ensure that the quality requirements are met by the inspection bodies and certification bodies. As part of this accreditation procedure, an accreditation body would verify whether the inspection body and the certification body are (still) compliant with the requirements set out above in terms of qualifications and independence. This would guarantee that the certification bodies are suitably qualified to carry out their duties and would establish legal certainty for cloud service providers and cloud service users alike.

In the interests of a functioning internal market and a standardised level of data protection, this accreditation should be valid for the entire area covered by the EU General Data Protection Regulation. This would mean that an inspection body could, based on its accreditation, carry out inspections within the entire jurisdiction of the Regulation, while a certification body could determine whether to award certificates within the same jurisdiction. In addition, this would ensure that the territorial jurisdiction of the accreditation would overlap with that of the certification because the certificate should also be valid throughout the EU.

Accreditation should be performed by bodies that are suitably qualified, in particular technically qualified to do so. For this purpose, the EU General Data Protection Regulation should stipulate the requirements that are to be met by these regulation bodies, but should allow the individual member states to nominate the accreditation bodies. It would not be advisable to have accreditation bodies designated at European level directly, as this would greatly undermine the competence of the member states in terms of administrative organisation.



5 — Revoking certification, liability and legal recourse

→ Revoking certificates

If a certified service no longer fulfils the requirements for the awarding of a certificate or if it comes to light that the requirements were not fulfilled from the outset, the continued validity of the certificate is then called into question. In cases where (essential) requirements were not met from the outset, and also in cases where the requirements are no longer fulfilled, the certificate (no longer) reflects the facts of the situation and therefore should never have been awarded or can no longer be awarded to the service. While minor changes are irrelevant in either scenario, the consequences of major deviations is open to question.

Cloud providers should be prohibited by law from continuing to make use of a certificate that has been revoked. To enable the certification body to revoke a certificate where changes make it necessary to do so, the cloud service provider must be obliged to notify the certification body when the cloud service provider determines that (essential) aspects of the service have changed or are changing. This obligation should be enshrined in law. If the certification body receives a notification of this kind, it must then examine the facts of the situation to determine whether the certificate should be revoked or whether the service continues to fulfil the requirements under data protection legislation – for example, because the cloud service provider immediately redresses the deficiency. If the cloud service provider is obliged in this way to provide notification in the event of changes, resulting in an obligation on the part of the certification body to repeat its inspection,

this means that a certificate does not provide a static snapshot assessment of a cloud service, and instead enables a dynamic process of continuous quality control. To ensure that cloud service providers can be relied upon to meet their obligation to notify the certification body of changes to services, failure to do should be sanctioned in an appropriate manner. The cloud service user's trust in the certificate must be protected until such time as it is revoked. Cloud users should only have reason to lose their confidence in certificates if these are revoked, in which case the users are themselves responsible for verifying the cloud service provider's compliance with data protection requirements and for switching cloud service providers if necessary. This principle should be explicitly enshrined in law. This protection of trust reinforces the acceptance of certifications, which in turn promotes data protection and data security because certified services offer a much greater objective assurance that data protection requirements are being fulfilled. It is also essential for a certificate to be revoked if it subsequently comes to light that the cloud service did not, from the outset, fulfil the requirements under data protection legislation and therefore should never have been awarded a certificate.

This is important because cloud service users place their confidence in the certificate in this case also and assume that they can safely avail of the cloud service. If, for example, the certification body determines, on the basis of a notification by the cloud service provider or a report from a cloud service user, that the requirements on which award of the certificate was based were not (at any stage) fulfilled by the service, the certification body must revoke the certificate and must publicise this revocation in the same way that it originally publicised the awarding of a certificate for the service.

The revocation of the certificate must not have any retroactive effect, and should only be effective for the future because it is essential for cloud service users to be able to place their trust and confidence in the existence of a certificate. However, for quality assurance reasons and bearing in mind that the unjustified awarding of a certificate may have been due to a breach of data protection legislation, it is necessary for provision to be made for a penalty to be imposed in respect of liability.

→ **Liability in the event of incorrect certification**

Certificates may prove to have been awarded incorrectly. Certification is incorrect if, contrary to the statement made on the certificate, the certified service either does not fulfil or ceases to fulfil the requirements under data protection regulation. Damages to the cloud service provider, cloud service users or other affected parties may arise in the event of incorrect certification. This raises the question of whether claims for damages can then be made against the certification body.

Damages due to incorrect certification

If a cloud service is awarded a certificate even though it does not fulfil the requirements, this results in cloud service users availing of a service that is not compliant with data protection legislation. In this context, damages to the cloud service user may arise as a result of incorrect certification. This is the case, for example, if a cloud service user is forced to switch cloud service providers because of a non-compliant cloud service and if costs are incurred by the cloud service user as a result, or if actions taken by the regulatory authorities result in costs, or if, in an extreme case, a fine is imposed due to unauthorised data processing (although the existence of a valid certificate will normally exonerate the cloud service user from fault, see above).

If unauthorised data collection, data processing or data use occurs as a consequence of incorrect certification, and if damage is incurred by affected parties as a result, these affected parties are also entitled, in principle, to make a claim for compensation against the cloud service user in accordance with Section 7 sentence 1 of the Federal Data Protection Act. However, according to Section 7 sentence 2 of the Federal Data Protection Act, the obligation to pay compensation does not apply if the cloud service user has exercised all due care required by the circumstances. It can be assumed that the cloud service user has done so by using a certified cloud service (see Point II.2). If the cloud service user avails of a certified service, the cloud service user is not ordinarily liable for breaches of data protection that occur because the cloud service does not in fact fulfil the requirements under data protection legislation. If the certificate was incorrectly awarded as a result of a defective inspection by the certification body rather than the provision of false data by the cloud service provider, liability on the part of the cloud service provider is usually to be ruled out because the provider can hardly be charged with a culpable breach of duty in this case either. After all, if a certificate is awarded, the cloud service provider may assume that the service provided is in compliance with statutory provisions. The only exception would be a situation in which the cloud service provider is aware or must be aware that the service is not compliant with data protection legislation despite being successfully certified.

Damages to the cloud service provider also cannot be ruled out in the event of incorrect certification because the cloud service provider will usually have additional expenses to pay and may lose customers. The decision as to whether a claim for damages can be made against the certification body in such an instance can most likely only be made on a case-by-case basis because the damages could be interpreted as stemming from the cloud service provider itself offering a service that is not compliant with data protection legislation.

Liability due to incorrect certification

If damages to the cloud service provider, cloud service user or other affected parties arise as a result of incorrect certification, the certification body or inspection body may be found to be liable on a number of different legal bases.

Contractual liability is only likely to arise in connection with the cloud service provider because only the cloud service provider has a contractual relationship with both the inspection body and the certification body. It is also not guaranteed that these contracts are to be regarded as contracts with a protective effect benefitting the cloud service user or even the affected party. In any case, the legal institution of contracts with a protective effect to the benefit of third parties is not recognised in every member state. It is therefore necessary to put a statutory regulation in place in relation to the liability of the inspection body and the certification body in the event of an incorrect inspection/incorrect certification.

If certification is found to be incorrect, claims for damages by cloud service providers, cloud service users and other affected parties come into consideration – provided that a corresponding statutory regulation is in place. In view of the provision in Section 8 of the Federal Data Protection Act, which imposes strict liability (although only for public bodies), it would appear that, even in the case of an incorrect inspection or certification, strict liability is not to be excluded from the outset. However, as long as liability of the cloud service provider and the cloud service user is exclusively fault-based (compare Section 7 sentence 2 of the Federal Data Protection Act), strict liability for incorrect inspections or certifications would most likely be disproportionate. In this context, the EU General Data Protection Regulation or a delegated act should include a provision whereby the liability of the inspection body and the certification body is dependent on a culpable breach of duty.

The liability of the inspection body or certification body would accordingly presuppose that these bodies had either intentionally or negligently been in breach of their duties. This means that liability may result from an incorrect inspection of the cloud service on the one hand, or from an incorrect decision regarding the awarding of a certificate on the other. In each case, the critical factor is a breach of duty. The primary duty of the inspection body is to conduct a legally compliant inspection of cloud services based on

the applicable inspection requirements. It would therefore appear to be essential to define the requirements underpinning a legally compliant inspection as precisely as possible. Given that a specific legal provision does not yet exist for this purpose, one should now be established for the internal market as a whole.

The first responsibility of a certification body is to dutifully exercise its judgement in determining whether to award a certificate based on the inspection carried out by the inspection body. Liability arises in cases where a certificate was awarded incorrectly or where an awarded certificate was not revoked even though the requirements for awarding the certificate are no longer fulfilled.

The definition of a maximum liability limit in the legislation could be considered as a means of limiting the liability of inspection bodies and certification bodies. In addition, inspection bodies and certification bodies can protect themselves by concluding liability insurance contracts. Indeed, the legislator could make it a legal requirement for these bodies to have an adequate level of liability insurance cover.

In the event of an incorrect certification, the civil liability of the certification body could be reinforced by the powers of public authorities. In this regard, both the imposition of obligations on the inspection and certification bodies by the regulatory authorities and the imposition of penalties based on a classification of facts constituting an administrative offence (to be created for this purpose) are conceivable.

→ Legal recourse

If the certification body refuses to award a certificate, awards a certificate subject to restrictions (e.g. for specific protection categories only) or revokes a certificate, the cloud service provider must be afforded the opportunity, in its own legal interests, to conduct a judicial review of the decision made by the certification body. In contrast, it appears doubtful that third parties, such as cloud service users, affected parties, competitors or regulatory authorities, will have the right to appeal a decision made by the certification body. In fact, there would appear to be other, preferable ways of giving third-party interests due consideration. While most cloud service users and affected parties should already be sufficiently well protected against the possibility of liability on the part of the certification body, regulatory authorities can, in the event of incorrect certification, take action, where necessary, against the certification body by imposing orders or penalties on it. The type of legal recourse (i.e. civil law or administrative law proceedings) open to a cloud service provider depends on whether the dispute falls under private law or public law

(see Section 40(1) of the Administrative Procedure Code. This, in turn, depends in particular on the legal nature of the certificate, in other words, it depends on whether the certificate has been drawn up under private or public law. A key factor here will be the more precise

specifications provided by the future EU General Data Protection Regulation. Since the type of legal recourse may differ between one member state and the next depending on the national legislation, the General Data Protection Regulation should only require member states to allow for legal recourse against the denial, restriction or revocation of a certificate. Meanwhile, the individual member state should determine which form of legal recourse can be used.

6 Conclusion

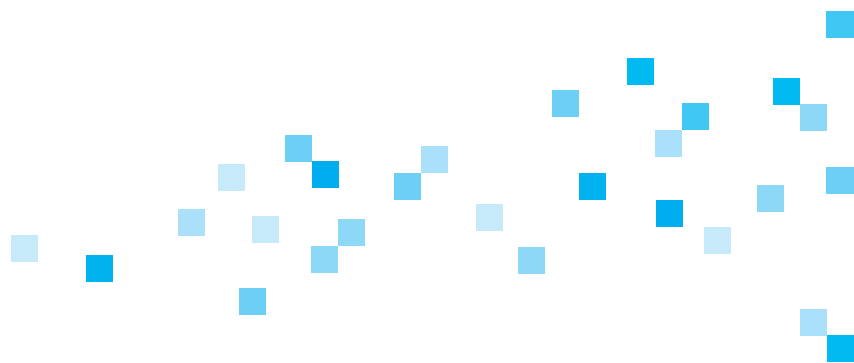
Data protection certification has the potential to be a very successful model for ensuring data protection in the context of the provision and use of cloud services. In particular, it enables efficient verification of the compliance of cloud services with data protection legislation, thereby reinforcing data privacy.

Successful data protection certification demands a robust and highly efficient certification procedure that guarantees fulfilment of the requirements for a compliant inspection and certification of cloud services, while also making certification affordable.

Because the certification procedure is of central importance to data protection certification, the European legislator should regulate the key principles of the certification procedure. In doing so, particular attention should be paid to the following aspects discussed in this paper:

- Inspection and certification based on uniform standards and rooted in legislation
- Validity of certification throughout the internal market
- ECloud users fulfil their verification obligation by inspecting the certificate
 - Cloud users' trust in the certificate is protected
- Inspection bodies and certification bodies are separate entities with separate sets of responsibility
- Inspection and certification are carried out by accredited inspection bodies and certification bodies
 - Inspection bodies and certification bodies are selected and commissioned by cloud service providers
- Inspection bodies and certification bodies are accredited by suitable accreditation bodies
- The certificate is withdrawn if the requirements are not fulfilled
- Liability of the inspection body and certification body in the event of a breach of duty

Data protection and efficient provision and use of cloud services can be achieved with equal effectiveness by implementing this type of high-quality, efficient data protection certification procedure.



Contributors/Authors

Prof. Dr. Georg Borges, Trusted Cloud Competence Centre, Saarland University
Oliver Berthold, Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und 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)
Claudia Husz, regio iT GmbH
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) Jan Lichtenberg, Deutsche Telekom AG
Peter Niehues, regio iT GmbH
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)
Dr. Christoph Sutter, TÜV Informationstechnik GmbH
Karin Vedder, Data Protection Supervisory Authority of Bavaria (Bayerisches Landesamt für Datenschutzaufsicht)
Dr. Thilo Weichert Independent Data Protection Centre for the State of Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) Monika Wojtowicz, TÜV Informationstechnik GmbH
Ursula Zabel, Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit)

Impressum

Herausgeber

Kompetenzzentrum Trusted Cloud

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

E-Mail: kompetenzzentrum@trusted-cloud.de

www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung

A&B One Kommunikationsagentur, Berlin

Druck

DCM Druck Center Meckenheim

Stand: April 2015

