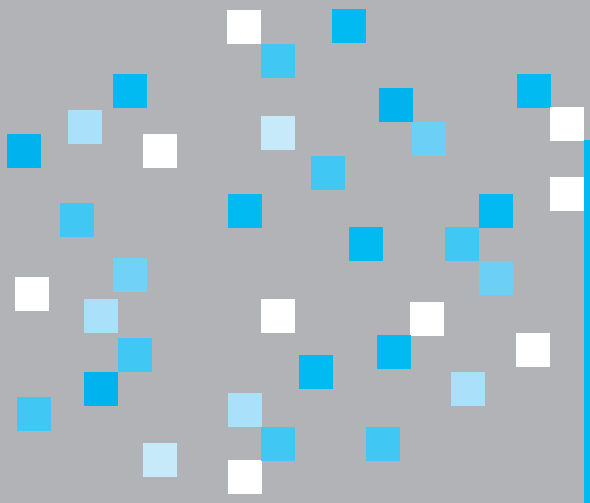
Trusted Cloud



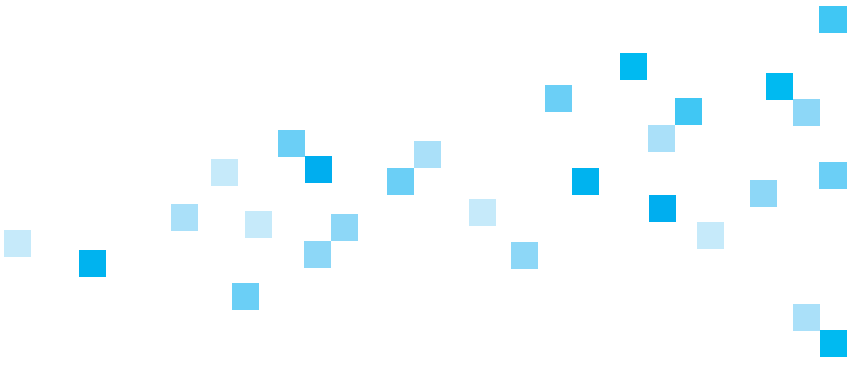
# Cloud Computing: solutions in the field of data protection law

Cloud Computing Legal Framework Working Group

## Working Group: The Legal Framework of Cloud Computing

The Working Group “The Legal Framework of Cloud Computing” in the Competence Center Trusted Cloud deals with legal aspects of cloud computing, with the goal of promoting the establishment of a reliable and adequate legal framework for cloud computing.

Members of the Working Group include representatives of the projects of the technology programme Trusted Cloud as well as renowned experts from the economic and scientific fields and the public sector. The Working Group is headed by Prof. Dr. Georg Borges.



# Cloud Computing: solutions in the field of data protection law

Cloud computing raises difficult issues in terms of data protection law. Not least, this applies to the rules governing the outsourced data processing used in cloud computing. This is largely because the existing rules on outsourced data processing are lagging behind the current technical developments in data processing (internet, cloud computing).

The forthcoming reform of European data protection law offers an opportunity to bring the law on outsourced data processing into line with the new technical and organisational conditions of data processing in the internet and in cloud computing.

This paper postulates 10 arguments in the interest of reforms to the law on outsourced data processing, and sets out a specific proposal for reform. The first part (arguments 1 – 5) sets out the reasons why the legislation needs to be reformed and develops the core element of the necessary reform, i.e. how a certificate system can cover the client's obligation to inspect the service provider. The second part (arguments 6 –10) describes the individual elements of this certificate-based solution.

# Argument 1

## The outsourced processing of data is a major way in which new forms of data processing take place.

The way electronic data processing is organised is undergoing a fundamental change due to modern technologies, and especially the internet. This change is manifested particularly clearly in the case of cloud computing.

In terms of data protection, the central characteristic of cloud computing is that the data processing is structured as a service. Correspondingly, the NIST (National Institute for Standards and Technology)'s definition of cloud computing distinguishes between three categories of service models: "software as a service", "platform as a service" and "infrastructure as a service". As the term itself implies, such a service is provided by another party. For this reason, in the case of cloud computing and other technical services, the substantive data processing on the one hand and the technical data processing on the other are often delivered by different parties.

Cloud computing is regarded as a dominant technical trend in data processing. In principle, it can cover the entire spectrum from data processing by companies of all sizes to data processing by government administration and private individuals. Cloud computing seems to be a logical next step in data processing in the age of the internet. Just as the physical location of the communication partner becomes insignificant when communication takes place via the internet, in the case of cloud computing, the place where the data is stored and processed becomes insignificant – at least in technical terms.

In the current German laws on data protection, the distinction between data processing as a technical process and substantive data processing is largely covered by the legal concept of outsourced data processing (Section 11 of the Federal Data Protection Act). This also applies to the draft of the General Data Protection Regulation, which distinguishes between the "controller" and the "processor".

If, therefore, it is the case that cloud computing and thus the organisational distinction between data processing as a technical service and the substantive control and use of the data processing will in future dominate the reality of data processing, this implies that outsourced data processing will become a typical instance of data processing to be covered by data protection law.

# Argument 2

**Some of the rules on outsourced data processing, in particular the requirements regarding contracts and the control the client exerts over the processor, are out of step with modern forms of data processing and need to be revised.**

The statutory rules governing outsourced data processing were originally set up with a view to covering major IT outsourcing projects, and are thus tailored to a situation which differs from present-day and future technology.

## → Outsourced data processing and IT outsourcing

Traditional IT outsourcing projects generally last a long time, are frequently on a large commercial scale, and are normally of crucial importance for the company outsourcing the work, as it is handing over a vital pillar of its operations to another party. A typical case of traditional IT outsourcing is a situation in which a company which has run its own computer centre in the past decides to outsource the data processing to another party.

The statutory rules governing outsourced data processing are designed to cover the needs of traditional IT outsourcing, and are characterised by the following main features:

- permissibility of outsourced data processing without the approval of the data subject;
- primary responsibility of the client for the data processing with respect to the data subject;
- restricted responsibility of the processor vis-a-vis the data subject (processor is primarily responsible for the security of the data processing);
- right of the client to issue instructions;
- comprehensive statutory requirements to be met by the contract between the client and the processor;
- duty of the client to exercise care in selecting the processor and to repeatedly monitor the data processing by the processor.

## → Data processing by service providers in the internet and cloud computing

In the age of the internet and cloud computing, the role played by third parties in data processing can be substantially different from that in traditional IT outsourcing.

Unlike traditional IT outsourcing, the use of cloud computing services is not necessarily a sizable project of major significance, but can also involve routine data processing similar to the way the internet is used. In such cases, cloud computing services are offered as standardised services.

The use of cloud computing services can also be on a small scale or on a temporary basis, e.g. in order to cope with periods of peak demand. In line with the NIST definition, cloud computing should be able to take place with minimal management effort, i.e. it should be possible to use it at short notice.

Even if traditional IT outsourcing can take place via the use of cloud computing, major new fields of application of cloud computing are the diametrical opposites of traditional IT outsourcing: in the one case, the vital significance of a single outsourcing procedure, the large volume of the transaction, substantial negotiations; in the other, also routine business, standard services, small-scale services, temporary services, short-term use of the service.

The differing nature of these applications of cloud computing can be illustrated by the difference between “made-to-measure” (traditional IT outsourcing) and “off-the-peg” (cloud computing for all).

Certain features of the statutory rules on outsourced data processing are oriented towards traditional IT outsourcing. As a result, many of the rules do not fit in with new forms of data processing. This is true both of the wide-ranging requirements to be fulfilled by the contract, and of the control to be exercised over the processor.

### → Need for reform regarding the clauses to be contained in the contract

The Federal Data Protection Act imposes comprehensive material and formal requirements on the contract governing the outsourced data processing, such as “written form”, which is interpreted to mean that the contract must be a physical document and signed personally. Overall, these requirements mean that a lot of effort is involved in concluding contracts on outsourced data processing. This effort was not a problem when it came to the traditional IT outsourcing of large projects.

However, these requirements do not fit the conditions of modern data processing, where the normal case is that a wide range of data processing services from various providers are used. In particular, the rules do not fully suit the concept of cloud computing, a feature of which should be “minimal management effort”.

### → The obligation that the processor be controlled by the client

Pursuant to Article 11(2) sentence 4 of the Federal Data Protection Act, the client must verify that the processor has taken the necessary measures to guarantee technical security. This obligation includes an on-site inspection of the technical and organisational measures. It is not clear whether the client has to undertake the on-site review in person, as some have advocated. In particular, it is not clear what measures can replace the personal on-site review by the client.

An on-site review by the client or his agent fits the reality of traditional IT outsourcing, in which a specifically defined computer centre or specific server formed part of the service.

However, this situation no longer applies even in the simple case of the use of email accounts or webspace. In particular, the idea that the client should supervise aspects like the security of individual servers or rooms containing servers is unrealistic in the age of cloud computing. The advantages of modern forms of data processing derive from the joint use of technical resources for different data processing procedures in which many users access one computer or server, or several servers or computer centres are used in parallel.

This reduces the idea that the client should conduct an on-site inspection to an absurdity, since he would need to visit a large number of sites, without even ultimately being sure whether a particular site is actually being used or not. It is true that it is possible to inspect several sites, but the transaction costs rise so much that they at least partially outweigh the efficiency gains deriving from the distributed data processing.

On the other hand, there would be fears of on-site inspections of cloud computing providers by a large number of clients ("inspection tourism"), which the processor would not be able to cope with, neither financially nor physically. Also, a large number of inspection visits to the computer centres by clients would undermine fundamental requirements for security and data protection.

Furthermore, it would be necessary to ask to what extent small and medium-sized clients would be capable of conducting a professional evaluation of the measures taken by the processor.

### → Need for reform

The current requirements imposed by the Federal Data Protection Act on the contract and on the control of the processor by the client result in excessive transaction costs for the use of modern forms of data processing, meaning either that the desired economic advantages cannot be realised or that the statutory requirements are not observed in practice.

For this reason, the statutory rules on outsourced data processing should be reformed in such a way that the statutory requirements can be met with a reasonable amount of effort under the conditions of modern forms of data processing without lowering the material standard of data protection.

# Argument 3

## The primary legal responsibility of the client for outsourced data processing remains appropriate in the age of the internet and cloud computing.

The basic concept of outsourced data processing still fits modern forms of data processing. In technical terms, the use of cloud computing services is an internal procedure within the data-processing body, just as in traditional IT outsourcing. It seems appropriate for data protection law to permit such data processing.

If the use of the outsourced data processing were to be tied to approval from the data subject, this would have a major impact on companies' freedom to organise their own activities, and this in itself would also pose legal problems. In particular, it appears appropriate for companies and other organisations to be able to organise their data processing as they desire.

The primary accountability of the client to the data subject and the supervisory agencies is a necessary and appropriate consequence of the circumstance that the data processing by the technical service provider is regarded as an internal process of the client. If the client were to be relieved of this responsibility, the data subjects' interest in being protected would be significantly impaired.

The restricted responsibility of the technical service provider as the processor therefore also seems appropriate. If the processor were to be the full addressee of the data protection requirements, the data subject would be able to enforce rights like the right to information and deletion, etc., directly against the processor. Since these rights can also be enforced against the client, this would result in difficult problems of co-ordination between the client and the processor. The fact that the technical service provider can normally only obtain the information about the permissibility of the data processing, such as the approval of the data subject, via the client, also creates a difficulty.

On the other hand, the supplementary responsibility of the processor for technical security, as anchored in existing law, does seem to be justified. The ensuring of the technical security of the data processing is carried out by the service provider, and the client can only influence it indirectly. It therefore appears correct to extend the responsibility for the technical security to the service provider and thus to make him a direct addressee of data protection law, as envisaged by current law and also by the EU's draft General Data Protection Regulation.

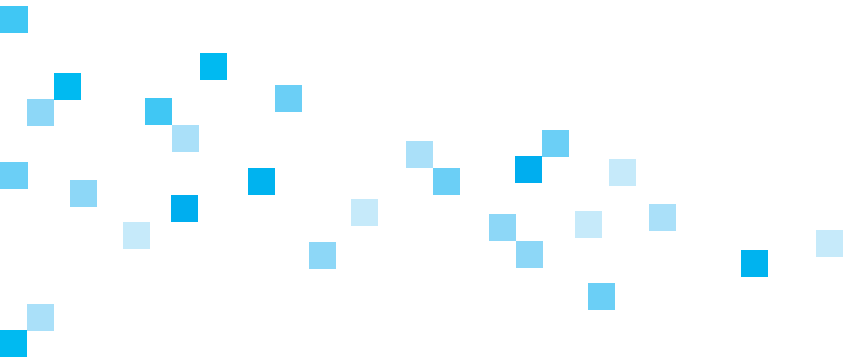
# Argument 4

**The clauses to be contained in the contract governing outsourced data processing must be shaped in such a manner that much of the mandatory content of the contract can be prepared by the processor and, for example, agreed to via web-based forms.**

There is a need to reform the statutory requirements imposed on the contract governing outsourced data processing. This applies not least to the requirement of Section 11 (2) sentence 2 of the Federal Data Protection Act that the contract be in writing (i.e. a physical document). In view of alternative possibilities to document the assurance of an adequate level of data protection, the written form as defined in Section 126 of the Civil Code does not appear necessary, at least de lege ferenda. Like the EU Data Protection Directive of 1995, the draft EU General Data Protection Regulation dispenses with the requirement that contracts be in writing and deems it sufficient to document the contract. The statutory requirements imposed on the content of the contract must be shaped in such a way that they can principally be fulfilled online. Here, it should be borne in mind that numerous services to reduce transaction costs are offered by processors as standardised services; this is the norm for renting storage space and for numerous cloud computing services. In this case, the client must be able to comply with the contract content requirements by undertaking a reasonable effort. This is the case for example if the processor prepares a form with the prescribed content of a contract on outsourced data processing – including the right to issue instructions – which is then completed by the user, the responsible body, who inserts the specific details. In this procedure, the contract takes the form of a text, and this is sufficient for the purposes of documentation.

In practice, this approach will be used for standardised services. When it comes to more complex services, and especially to customised services, the contract will be drawn up specifically for that case and concluded in a different manner.

The possibility to comply with the statutory requirements by means of web-based forms, dispensing with paper forms, should be explicitly permitted by the Act in order to ensure clarity of the law.



# Argument 5

**The main problem of the requirement to exercise control can be resolved if the inspection by the client can be substituted by a certificate produced by an independent third party which certifies that the inspection has been carried out as required by law. The possibility to substitute the inspection by a certificate should be stipulated in the Act.**

There are various ways to resolve the difficulties linked to the requirement to exercise control, ranging from the repeal to the modification of the requirement.

### → Gaps in protection if no controls are required

Abolishing the requirement to exercise control would mean that the obligations of the client would be limited to the selection of an appropriate processor and the conclusion of a contract requiring the processor to meet the statutory data protection requirements. This would, however, create gaps in protection, since the processor is only partially addressed by the data protection requirements.

In particular, if no controls are carried out, it would not be possible to prevent unreliable processors, which claim to act in conformity with data protection rules and can thus be selected by the client, whilst actually failing to comply with the data protection rules, from being entrusted with data processing.

### → Liability is no substitute for control

Another solution would be for the client to be required to assume liability. Here, the client would have to assume full liability for the processor, as envisaged by Section 11 of the Federal Data Protection Act. In this case, the client would have his own interest in supervising the processor due to the risk of liability.

In principle, the concept of using liability to steer behaviour, as is found in civil law, is persuasive. However, it is not at present a persuasive option in data protection law, since the use of responsibility under civil law to steer behaviour is not effective at present in the field of data protection. Since it is difficult to calculate the level of damages, the liability for violations of data protection rules, which is already contained in a strict wording in the Federal Data Protection Act, has so far lacked any significant meaning in practice.

### → Modification of the supervisory duty

For this reason, it seems reasonable to modify the control obligation in order to overcome the weaknesses.

As already stated, a central problem of control in modern data processing is the fact that the individual user uses many different systems, and at the same time that a large number of users use the same resources, so that in the case of outsourced data processing every user would have to control a large number of data processing systems, and individual systems would have to be controlled by a large number of users.

This structural problem can be overcome by pooling control. In the ideal case, each system should be inspected by an independent body, and the inspection should benefit all of the users.

Such a pooled inspection is already possible de lege lata. The inspection required pursuant to Section 11(2) sentence 4 of the Federal Data Protection Act does not have to be carried out by the client himself, but can be undertaken by an independent third party. The third party can carry out one and the same inspection on behalf of several clients as long as this inspection covers the necessary aspects for each client.

There is currently a debate about whether the control can be exercised by the processor, e.g. on the basis of a detailed questionnaire from the client. However, this suggestion is countered by the point that a control is an inspection carried out by someone other than the inspected party. Also, self-inspection could not prevent the emergence of unreliable providers.

Increased state supervision of cloud service providers cannot replace the specific inspection of the processor, nor can it avoid the risks of any self-inspection, since capacity constraints will not permit data protection authorities to carry out a full inspection of all processors.

For this reason, the best solution appears to be inspections by independent third parties. These third parties would have to guarantee their ability to carry out an appropriate inspection, i.e. in particular they need to document their professional qualifications.

The inspection would have to be documented. In outsourced data processing, the respective client could demonstrate that an inspection has taken place via documentation from third parties, such as the supervisory authority.

Such inspection documentation can be concluded by a certificate from the inspector confirming that the statutory requirements to be met by the processor have indeed been fulfilled.

The inspection by independent third parties can also be initiated by the processor. In other words, it is possible for the processor to have an inspection carried out and to provide the client with the documentation and the certificate of the inspection; this would mean that the client no longer needs to carry out the statutory inspection of the aspects covered by the certificate unless he has specific grounds for doing so.

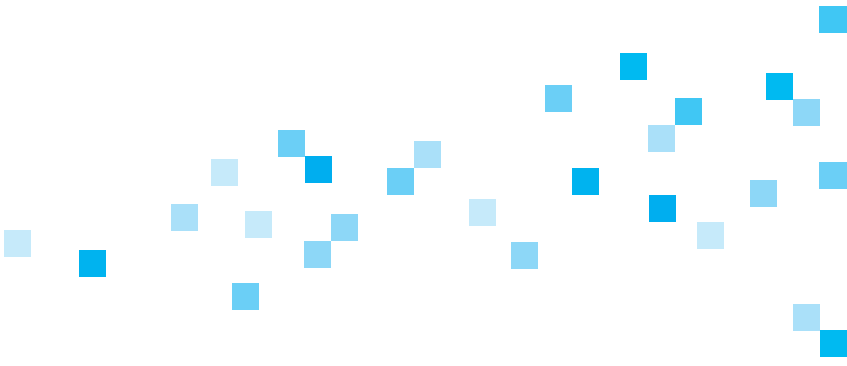
Such a certificate would have to be renewed on a regular basis, just as the client's personal inspection has to be carried out at regular intervals. Elements like ongoing reports (monitoring) could also be documented in the form of certificates, and could be an element of the official certificate if there is a statutory obligation for this.

This means that the inspection required by law can be replaced by the certificate of an independent third party as long as the inspection which has been documented in detail and confirmed by the certificate covers the necessary controls to be exercised by the respective client.

### → Need for clarification of the law

The possibility to replace a personal inspection with a certificate from an independent third party in the context of Section 11(2) sentence 4 of the Federal Data Protection Act is already in line with the prevailing opinions of academics and practitioners. However, there is still a considerable degree of uncertainty with respect to the legal consequences of the certificate, and especially as to whether the existence of the certificate means that personal inspections by the client are no longer required. In particular, the requirements to be met by such a certificate are unclear.

For this reason, a revision of the legislation is necessary to state explicitly that – within the preconditions to be defined by law – the client's duty to carry out controls can be replaced by the presentation of a certificate from an independent third party on the implementation of the inspection required by law. This is without prejudice to the duty to carry out inspections where there are specific grounds to do so.



# Argument 6

## The certificate shall cover the client's inspection of the processor as required by law, on the basis of a standardised catalogue of requirements.

The subject-matter of the certificate must derive from its function. The content of the inspection which is to be replaced by the certificate is that the technical and organisational measures taken by the processor comply with data protection legislation.

The necessary technical and organisational measures shall be oriented towards the individual case and must be determined by weighing the need for protection against the effort required to achieve it. For this reason, it is not possible to set down a general stipulation of the measures required by law for each individual case.

However, this does not exclude the possibility of a single certificate for a cloud computing service. Firstly, it should be borne in mind that a large proportion of the technical and organisational requirements will be the same for a large number of data processing procedures. By way of illustration, the requirements for secure access to rooms containing servers will be the same, no matter whether the accounting data being processed is from a butcher or a baker. This means that similar requirements can be formulated for most fields of application.

The law prescribes a minimum standard for the technical and organisational measures, and does not exclude the possibility of higher standards. For this reason, the divergences which would emerge if the requirements were assessed on a case-by-case basis can be offset by issuing a certificate which confirms a high level of protection, so that it can be safely assumed that the statutory requirements to be met by an individual case are indeed fulfilled.

Consequently, the certification procedure can result in a higher standard of data protection, and this can be a further incentive for the client to use a cloud solution. The burden imposed on the providers of outsourced data processing is not increased further, since they will, anyhow, aim for a uniform level of protection for the sake of efficiency, and they will therefore opt for a high level of protection in order to meet the needs of differing groups of customers.

The statutory requirements imposed on the technical and organisational measures are summarised in a catalogue of requirements governing the practical implementation of the inspection; this serves as the basis for the inspection and thus the certificate. The certificate covers the inspected measures. This can cover the statutory requirements for standardised cloud services and standardised data processing.

To the extent that the client has to observe special statutory requirements, particularly with regard to the nature of the data (e.g. health data) or the nature of the data processing, these are not normally covered by the certificate. It therefore remains necessary for the client to carry out inspections. However, even for these special applications, case groups will often be formed, and these can then again be the subject of a specific certificate (e.g. certificate for the outsourcing of the processing of health data). The same applies where the risk profile of the data processing is altered by special technical protective measures (e.g. encryption).

# Argument 7

**The criteria for the inspection which is required for certification must be stipulated uniformly by law for the European single market. The stipulation of the inspection criteria should take place via a procedure involving data protection authorities and representatives of providers and users of outsourced data processing.**

If the inspection of the service provider for the purpose of issuing a certificate is to take place on the basis of a standardised inspection catalogue, it is necessary to clarify which institution is to stipulate the inspection criteria contained in the catalogue(s).

The procedure to stipulate the inspection criteria should meet a series of fundamental requirements:

- The inspection criteria should be uniform for the single market, since otherwise the harmonisation intended by the Regulation will not be attained in this important respect.
- It should be possible to adapt the criteria to the changes in data processing so that the level of protection can still be attained even when technical or organisational changes occur.
- The criteria should be stipulated by an institution or in a procedure which involves the interests of all the stakeholders, in particular those of data protection and the providers and users of services.

These fundamental requirements help us to select the appropriate procedure:

- The theoretical possibility of having the inspection criteria determined by the certifying body itself does not fulfil the intended objectives. It would result in divergent requirements. Also, the certifying body would have an incentive to set the inspection criteria too low.
- In view of the objective of harmonisation, the determination of the inspection criteria should not be left to the individual member states.
- Stipulation of the inspection criteria in the Regulation itself would certainly result in a uniform arrangement. However, this would overburden the text of the Regulation, and in particular this approach would be too inflexible.
- The inspection criteria could be stipulated by means of a delegated act by the European Commission. However, the Commission lacks the requisite expertise for this. For this reason, the supervisory bodies and data protection experts from business and academia would have to be involved, so that use can be made of their expertise. Preference should therefore be given to solutions which ensure this involvement.
- The Regulation could commission the European Data Protection Committee (now: Article 29 Working Party) to stipulate the criteria. There are several arguments in favour of this. Under current law, the data protection authorities are already entrusted with supervising compliance with the statutory requirements, and therefore have a lot of experience and expertise. Also, these are bodies which are endowed with independence under the EU Data Protection Directive.

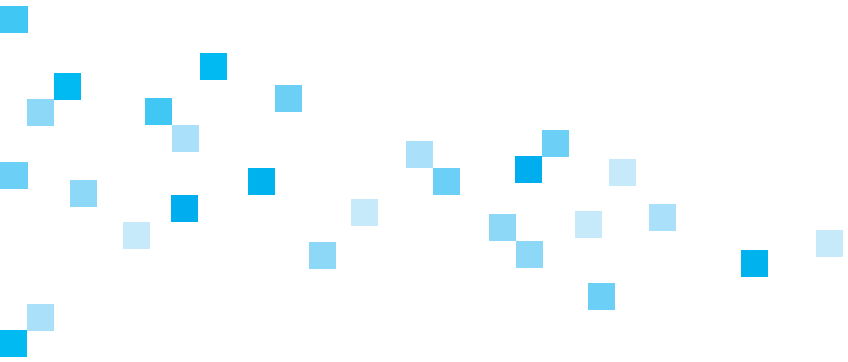
However, the stipulation of the inspection criteria by data protection authorities would not fully meet the interests of all stakeholders in shaping these criteria. In particular, the expertise of the users and providers of the services could not be included.

- A new institution in which all stakeholders are represented could be entrusted with stipulating the criteria. However, no such institution currently exists at the European level. The establishment of a new institution merely to stipulate inspection criteria does not seem to make sense.
- The criteria could also be co-ordinated in a procedure in which inspection criteria are stipulated by involving data protection authorities and other interest groups in a co-ordination procedure. This procedure could be administered by the European Data Protection Committee.

In functional terms, this approach is at least equivalent to stipulation by a separate institution, and it can make use of existing structures. At the same time, it would guarantee comprehensive involvement of all interest groups.

Ultimately it seems necessary to stipulate the inspection criteria at the European level in a procedure directly involving the expertise of all the stakeholders.

In organisational terms, it seems preferable to ascertain the inspection criteria via a co-ordination procedure involving the data protection authorities and the users. This co-ordination procedure should be administered by the European Data Protection Committee, whereby it is assumed that, in view of the importance being attached to the Committee by the draft General Data Protection Regulation, it will be equipped with the necessary administrative infrastructure.



# Argument 8

**It should be possible for the certificate to (also) be issued by qualified private bodies. The aptitude of the certifying body should be documented by accreditation. The certifying body should be liable for erroneous certificates.**

If it is to be possible for the inspection by the client to be replaced by a certificate, it is necessary to clarify which institution is to issue the certificate.

### → Issue of the certificate as a private-sector commercial activity

Here, it is necessary to bear in mind that the developments in data processing (internet, cloud computing) will probably result in a large number of outsourced data processing services which need to comply with data protection rules, and that it may therefore be necessary to issue a large number of certificates.

It is therefore necessary for there to be sufficient capacity to issue certificates. Simply for this reason, it would seem inadvisable to require the certificates to be issued by state bodies. Also, limiting this activity to state bodies would probably create legal problems. A market for certificate providers can develop if the issuing of certificates emerges as a commercial activity.

On this account, there is every reason to assume that the certificate can (also) be issued by private bodies.

### → The need for quality requirements to be imposed on the certifying body

If the certificates can (also) be issued by private bodies, it is necessary to clarify what requirements are imposed on the certifying body. One possibility would be to dispense entirely with statutory requirements being imposed on the certifying body and to ensure that an adequate inspection is carried out before the certificate is issued by making the certifying body liable for erroneous certificates. However, there are general weaknesses in the liability model in the field of data protection. Even if the certifying body is subject to criminal proceedings or administrative penalties when it issues an erroneous certificate, on its own this cannot ensure that certificates are only issued by qualified bodies. There is therefore a need for quality requirements to be imposed on the certifying body.

The General Data Protection Regulation should therefore explicitly stipulate the need for the certifying body to have the necessary expertise and staff to issue the certificate.

### → Using accreditation to ensure that the requirements are met

If the certifying body has to meet qualitative statutory requirements, it is necessary to clarify how the fulfilment of these requirements can be ensured. Once again, there are various ways to do this.

- There is a theoretical possibility of describing the qualification requirements to be met by the certifying body in general abstract terms in the Regulation, whilst dispensing with formal guarantees of compliance with the qualifications. In this case, it would be up to the client wishing to rely on a certificate to find out whether the certifying body meets the statutory requirements, since only if that were the case would the certificate be valid. However, the client cannot be expected to shoulder this risk. Also, many clients would lack the necessary expertise. The client needs to be able to rely on the body issuing a certificate being authorised to do so.
- Similarly, the possibility to reserve the right to issue certificates for a certain profession, or to make it dependent on a state examination, as with certified auditors for final audits pursuant to Section 319 of the Commercial Code, also appears rather theoretical. This requirement would appear to be excessive in the case of the certificate. On the other hand, it would be feasible to state in advance that certain categories of professions or bodies were suited to the task.
- The entitlement to issue a certificate could be made dependent on an inspection of the certifying body, e.g. via certification or accreditation. There are numerous instances of such an approach. Such an approach, whereby the certifying body is first inspected, and, if it meets the statutory requirements, is accredited, can provide the client with the necessary guarantee and legal certainty that the body is qualified to issue certificates.

For this reason, the aptitude of the certifying body should be ensured by means of an inspection required by law (accreditation).

### → Ensuring orderly certification via liability

The accreditation model can ensure that the certifying body meets the quality requirements. However, it in itself cannot guarantee the quality of the inspection leading to certification.

For this reason, the Regulation should also additionally provide for liability under civil law for erroneous certificates issued by the certifying body. The liability under civil law should be backed up by liability for inadequate certification under the law on administrative offences so that state bodies have the corresponding right to intervene.

# Argument 9

**The preconditions for accreditation of certifying bodies should be stipulated in a procedure by representatives of the data protection authorities and representatives of the clients and processors. The accreditation should apply to the entire area covered by the General Data Protection Regulation.**

If the accreditation is to be prescribed by law, it is necessary to clarify which preconditions need to be imposed on accreditation and which body sets out the details of the requirements.

Here, there are similar options to those for the stipulation of the content to be covered by the certificate. The objectives cited there, and in particular the uniformity of the requirements and the possibility to adapt them to new developments, should also apply to the requirements for accreditation.

### → Stipulation of principles in the Regulation

The stipulation of the requirements should not be left to the individual member states, but should take place at European level in order to ensure uniformity.

It seems inappropriate to provide a detailed stipulation in the Regulation of the requirements to be met by accreditation, since this would overload the text of the Regulation and would remove all flexibility from accreditation.

For this reason, the preconditions of accreditation should be described in a general form in the Regulation so that there is an adequate basis for the stipulation of the details.

### → Stipulating the details of the requirements

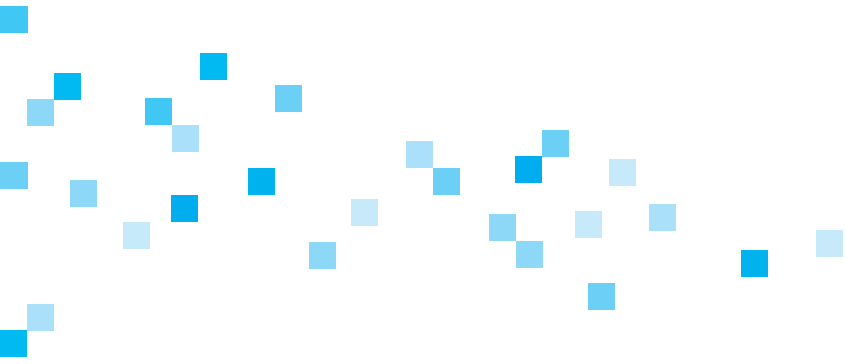
Assuming that the Regulation lays down the principles to be met by accreditation, it is necessary to clarify which body stipulates the details. This stipulation should be undertaken uniformly for the single market, since otherwise the requirements would no longer be uniform.

In line with the stipulation of the inspection criteria for issuing the certificate, it seems to make sense to stipulate the requirements to be met by accreditation in a procedure which draws directly on the expertise of the data protection authorities and of the clients and processors. Once again, this co-ordination procedure should be administered by the European Data Protection Committee.

### → Area of validity of accreditation

If the certifying bodies are to receive an accreditation in the single market, the question of whether the accreditation applies only to the home state of the certifying body or to the entire single market is important.

It therefore seems crucial for the accreditation to apply to the entire area covered by the Regulation so that the accreditation entitles the certifying body to issue certificates valid in the entire single market. Only then will the accreditation correspond to the area of validity of the certificate, which also applies to the entire area covered by the Regulation.



# Argument 10

**The accreditation should be undertaken by suitable bodies which have the necessary expertise and are independent. The Regulation should stipulate the basic requirements to be met by the accreditation bodies, and leave the designation of the accreditation bodies to the member states.**

To the extent that the certifying body needs to document its qualifications via accreditation, it is necessary to clarify which body should issue the accreditation. A direct stipulation, at the European level, of the bodies responsible for the accreditation, be it in the Regulation, via a delegated act by the Commission, or by the European Data Protection Committee, seems to present problems since it would intervene very strongly in the organisation of data protection, which is the responsibility of the member states. This is therefore not a feasible approach.

The requirements to be met by the accreditation body should be stipulated in general, abstract terms in the General Data Protection Regulation. The Regulation should state that accreditation can only be undertaken by bodies which have the specialist skills and independence, such as is to be found for example in data protection authorities.

It seems reasonable to leave the designation of the accreditation bodies to the member states, since the way that data protection is organised varies between the member states. The danger of divergent standards in the single market will be greatly reduced by the fact that both the requirements to be met by the accreditation and the responsibility in the case of erroneous accreditation will be regulated at European level. So this is more of an organisational question than one of divergent standards of protection.

## The Recommendation on Commissioned Data Processing

The recommendation “Solutions of Data Protection Law for Cloud Computing” was elaborated by members of the Working Group “The Legal Framework of Cloud Computing” under the leadership of Prof. Dr. Georg Borges and unanimously adopted by the entire Working Group in September of 2012.

The Working Group proposes that the concept described in the paper be implemented by the legislator.

### → Contributors

**Dr. Thorsten Behling,** KPMG Rechtsanwaltsgesellschaft mbH

**Josef Bergner,** Municipal Information Processing Baden-Franconia (Kommunale Informationsverarbeitung Baden-Franken)

**Prof. Dr. Georg Borges,** Ruhr University Bochum

**Mathias Cellarius,** SAP AG

**Dr. Alexander Duisberg,** Bird & Bird LLP

**Dr. Jens Eckhardt,** JUCONOMY Attorneys

**Alexander Glaus,** Deutsche Bank AG

**Björn Hajek,** Infineon Technologies AG

**Wulf Hartmann,** Association of German Banks, e. V.

**Dr. Marc Hilber,** Oppenhoff & Partner

**Dr. Hubert Jäger,** Uniscon universal identity control GmbH

**Kristian Klodt,** QSC AG

**Rudi Kramer,** DATEV eG

**Steffen Kroschwald,** University of Kassel

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

**Ulrich Lepper,** The Commissioner for Data Protection and Freedom of Information of the State of North Rhine-Westphalia (Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen)

**Ninja Marnau,** Independent Centre for Privacy Protection Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ULD)

**Dr. Jan Geert Meents,** DLA Piper UK LLP

**Matthias Rüdiger,** ITDZ Berlin

**Stephan Sädtler,** University of Passau

**Gunther Schiefer,** Karlsruhe Institute of Technology (KIT)

**Gabriel Schulz,** The Commissioner for Data Protection of the State of Mecklenburg-Western Pomerania (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern)

**Prof. Dr. Jürgen Taeger,** University of Oldenburg

**Barbara Trusch,** HSH Soft- und Hardware Vertriebs GmbH

**Dr. Claus-Dieter Ulmer,** Deutsche Telekom AG

**Thomas von Bülow,** 1&1 Internet AG

**Magda Wicker,** University of Kassel

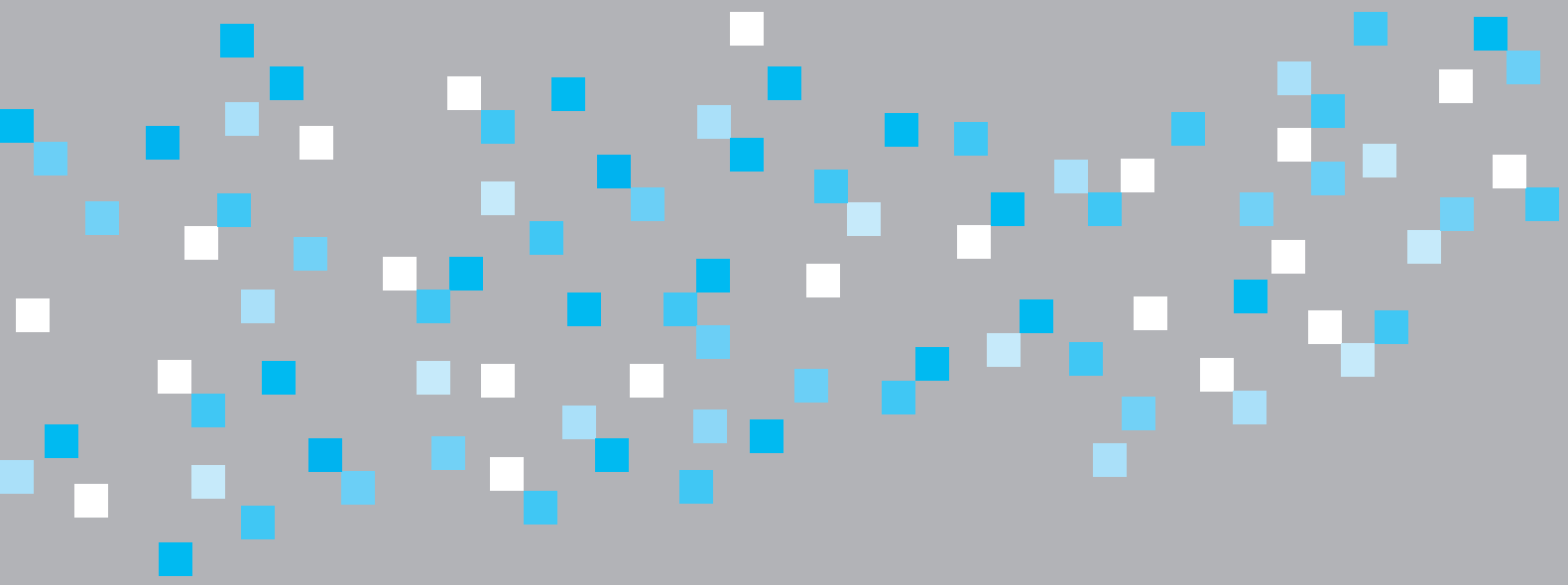
**Imprint**

**Editor**
Kompetenzzentrum Trusted Cloud
AG Rechtsrahmen Cloud Computing
Telephone +49 (0)30 880 04 22 01
e-mail: kompetenzzentrum@trusted-cloud.de
**www.trusted-cloud.de**

**Design**
A&B One Kommunikationsagentur, Berlin

**Print**
vierC print+mediafabrik, Berlin

Date of issue: October 2012



www.trusted-cloud.de