The Sedona Conference® Working Group Series℠

wgs℠

Cloud Computing & Data Privacy

Dr. Thilo Weichert
Independent Center for Data Protection
for the German State of Schleswig-Holstein

Translated from the German for The Sedona Conference®
by Lillian Clementi, Lingua Legal® Intelligent Translation
for Law & Business®

A Project of The Sedona Conference®
Working Group on International Electronic
Information Management, Discovery & Disclosure (WG6)

February 2011

The Sedona Conference®

Cloud Computing & Data Privacy

Dr. Thilo Weichert
Independent Center for Data Protection
for the German State of Schleswig-Holstein

Translated from the German for The Sedona Conference® by
Lillian Clementi, Lingua Legal® Intelligent Translation for Law & Business®

We wish to thank our Working Group Series℠ sustaining and annual sponsors
for their critical support of our mission.
A list of our sponsors is available on our website at:
www.thesedonaconference.org, under the "Sponsors" tab.

wgs℠

Visit www.thesedonaconference.org

Lingua Legal™ Intelligent translation for law and business™

AFFIDAVIT OF CERTIFICATION

The undersigned, Lillian S. Clementi, whose address is 2924 South Buchanan Street, Arlington, VA 22206-1547 USA, declares and states as follows:

I am well acquainted with the English and German languages; I have in the past translated German documents of legal and semi-technical content into English; and I hold a German-to-English translation certificate from New York University. Over the course of nearly 20 years, I have prepared and reviewed thousands of English language translations from German and French, and since 2004, I have served as managing principal of Lingua Legal, a language services practice providing translation and document review to clients in law and business.

I have been asked to prepare an English translation of the German document *Cloud Computing und Datenschutz* by Thilo Weichert.

I hereby declare that the attached translation of the text described above is, to the best of my knowledge and ability, a true and accurate translation of the original German document.

And I declare further that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that I am aware that falsification of these statements and the like is punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

I therefore attach this Certification of Translation to my English translation of this document.

Lillian S. Clementi, Translator
[Signature on file with The Sedona Conference®]
March 20, 2011

Cloud Computing and Data Privacy

Dr. Thilo Weichert

Independent Center for Data Protection for the German state of Schleswig-Holstein

Translated from the German for The Sedona Conference® by

Lillian Clementi
Lingua Legal®
Intelligent Translation for Law and Business®
www.LinguaLegal.com

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Independent Center for Data Protection for the German state of Schleswig-Holstein
(www.datenschutzzentrum.de)

Cloud Computing and Data Privacy

Thilo Weichert[1]

Using cloud computing to process personal data raises legal and technical questions that have yet to be adequately addressed. Because this form of data processing is increasingly popular, it is essential to define and articulate the data privacy principles that apply to it. In this analysis, we assume that the data are processed by private entities that are located in Germany and are subject to the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG). Processing by public entities within Germany's federal and state [*Land*] governments must generally meet similar standards under the BDSG and/or comply with the data privacy laws of the German states (*Landesdatenschutzgesetze*, or LDSGs).

1. Purpose und Types of Cloud Computing

Cloud computing has nothing to do with the weather. Rather, the term refers to the practice of outsourcing data processing to a still-nebulous landscape of computers connected via networks, and particularly via the Internet. Its goal is to offer dynamic, scalable use of information technology (IT) services—in other words, to allow customers to use outside hardware, software and know-how in order to *save resources*. Ideally, it should make no difference to users whether a task is performed by their own computer or a far-distant one. In some cases, entire processes are transferred to the cloud; in others, the goal is simply to cover peaks in demand that overtax in-house IT infrastructures. Customers generally pay a base rate plus additional fees scaled to their level of use and service, usually based on computing power and computer time. Flat rates are also a possibility.

This is not a new approach in IT: it has existed since the earliest days of data processing under the label *outsourcing*. In the context of data privacy law, it has been discussed under the concepts "contract data processing" and "function transfer." One current forerunner of cloud computing is grid computing, inspired by the idea of using networks to supply computing power much as water and electricity are supplied to consumers. But where the grid usually involves statically coupled computers, cloud resources are offered primarily on a flexible basis.

Within cloud computing, we *differentiate* among Software as a Service (SaaS), Storage as a Service, Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These, in turn, have given rise to

[1] Translator's Note: The German source document contained an inactive link to accompanying slides in German; it has been omitted from this translation. The slides and the original German paper can be found at https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html.

other concepts, such as HPC (High Performance Computing) as a Service. With SaaS, software is not installed on the customer's own computer, but is made available as needed via networks. Storage as a Service is used for data backup and archiving: data may be stored on a regular basis or via a one-time transfer. One special form of SaaS is replication services, which store data via the Internet, allowing access as needed. With PaaS, external users can access entire applications—a complete customer relations management (CRM) system, for example—while IaaS offers access to entire IT infrastructures.

Another term that goes hand in hand with cloud computing is *virtualization,* which means running a "virtual computer" on an external hardware platform, creating a logical separation between a given program and the operating system of the host computer.

Yet another term that crops up in this context is *service-oriented architecture* (SOA). Here, standardized business processes are mapped onto a heterogeneous mix of IT infrastructures that can be used to run cross-organizational processes. Because it is used most often in the context of web services, SOA uses XML standards, allowing data to be exchanged between independent organizations.

We can also draw a distinction between private and public clouds. A *private cloud* is a group of networked computers, all of which fall under the legal responsibility of a single data-processing entity. The private cloud category includes virtualized desktops, a special type of in-house cloud in which the data controller provides an operating system that employees can access via thin clients, mobile laptops, or PCs to access and process data. The private cloud category also includes computer networks formed by entities with a close legal relationship to one another, such as entities in government or within a corporate group.

Public clouds provide third-party computing power as defined by data privacy law (BDSG[2] § 3(8) sentence 2). These clouds are offered by huge global IT companies, such as Amazon (EC2), Google, Microsoft, IBM and Hewlett-Packard (together with Intel and Yahoo), which process data in worldwide networks of distributed servers and server farms owned by one or more providers.

In addition to these commercial providers, a number of public—primarily academic—institutions offer cloud computing. Hybrid clouds, which combine aspects of private and public clouds, use both internal and external resources. One special case is *community clouds*, in which a cloud infrastructure is used collectively, and members jointly specify and agree upon shared needs such as security, data privacy and other compliance requirements.

As for the *actors* involved, we can generally differentiate among the cloud user, the cloud provider and the resource provider. The cloud user is the entity that benefits from the computing power offered by cloud services. The cloud provider makes these services available to the user but may not be the same as the resource providers, which generally make their hardware or software resources available to the cloud provider so that they can be combined and offered to cloud users for data processing.

[2] Translator's Note: An English translation of the BDSG with amendments through June 2010 can be found on the website of Germany's Federal Commissioner for Data Protection and Freedom of Information. Visit www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87568/BDSG_idFv01092009.pdf.

2. Practical Problems and Legal Issues

As a practical matter, cloud computing presents a number of *technical challenges*. When network-based computing takes too long, the resources saved in one location are unavailable to another.

The core problem of cloud computing lies in guaranteeing the *integrity and confidentiality of the cloud user's data processing*, and this is true not only for personal data, but for any data that require confidentiality and integrity, such as business and trade secrets, research data, and any other data protected under intellectual property law. The goal is to prevent harmful, unauthorized access by third parties.

One central aspect of every cloud contract is the security of the data processing, including maintenance, error correction and defenses against attack and disruption. Due to liability concerns, responsibility for specific security measures must be clearly assigned. Cloud users and providers can agree on security commitments in *Security Service Level Agreements* (SSLAs), but providers continue to offer "cloudy" security guarantees. SSLAs generally resemble the terms and conditions of standard business agreements.

Legally, cloud computing services are supplied and used under a contract, which can raise a number of legal questions—such as liability, warranty claims, and copyright—that we cannot address in detail here. Cloud contracts cannot be assigned to any one category: they are hybrids combining elements of a lease agreement, a loan, and a service and/or work agreement (training, maintenance, and interface customization).

Archiving data in cross-border clouds has significant consequences for tax records. In principle, § 146(2) sentence 1 of the German Tax Code (*Abgabenordnung*, or AO) requires that tax records be maintained and stored in Germany. Under AO § 146(2a) (added on January 1, 2009), the relevant tax authorities may, upon request, allow these documents to be archived in a European Union (EU) or European Economic Area (EEA) member state with an administrative assistance agreement. The foreign tax authorities must agree, and the German tax authorities must have access to the documents. If the authorities grant their permission, AO § 148 allows *tax documents* to be stored outside the EU/EEA countries only if storage in Germany would present a hardship for the taxpayer and only if it does not affect taxation.

Under *commercial law*, accounting documents and business letters must be stored in Germany. Section 257(4) of the German Commercial Code (*Handelsgesetzbuch*, or HGB) establishes a statutory retention period of six or ten years. Use of cloud archiving is not explicitly prohibited.

Some cloud services (such as Google Apps) are offered directly to consumers, which requires compliance with national and international *consumer law*.

Cloud-based data storage also presents a problem for the investigation of *crimes and administrative violations* if the nature and location of the data processing prevent access by investigating and enforcement authorities.

Because cloud-based data processing raises so many legal questions for which statutory guidance has yet to be issued, the structure of the *IT agreements* governing these relationships is critically important.

3. Applicability of data privacy law in general

From the data privacy perspective, cloud computing is only relevant if personal data are processed (BDSG § 3(1)), *i.e.*, when the processed information can be linked to an identified or identifiable natural person—a human being—referred to by the BDSG as the "data subject." One group of data subjects can be the data controller's employees, who use the cloud in performing their work and whose data are processed as a result. Where usage data are concerned, specific employee data privacy law applies. In addition, cloud use routinely involves processing personal data, such as data for a business's customers, suppliers and other partners, and other persons that have no specific relationship with the cloud user.

Data privacy law does not apply when personal data are adequately anonymized. But *data regarded as anonymized* (see BDSG § 3(6)) can become re-identifiable through cloud processing because other cloud users, or the cloud and/or resource providers, have access to additional information that makes re-identification possible.

Insofar as the *concept of attributability to specific individuals* is relative and not objective, using a cloud can change the quality of data processing. With today's complex network connections, however, data that have not been clearly identified can be linked to an identifiable person without a disproportionately large expenditure of time, money and manpower. As a result, the mere act of processing data in a cloud is not enough to affect the applicability of data privacy law. We should assume that individual data records can generally be linked to people. The mere possibility of electronic analysis and integration into a potentially global network increases the odds that additional knowledge which could be used to identify the data subject will be present.

Use of *aliasing*—replacing the identifiers for a natural person with other characteristics (BDSG § 3(6a))—does not necessarily mean that data privacy law is inapplicable. However, this method can make it so difficult to identify the data subject that the level of privacy is sufficient to permit data processing.

4. Applicability of national data privacy laws

Clouds tend to be cross-border entities: there are no technical reasons for them to take territorial limits into consideration. This is not the case for data privacy law, which is bound to the place where the data are processed. Under the European Union's Data Protection Directive (EU DPD)[3], however, cross-border data processing should no longer present a legal obstacle within the European single market (EU DPD Art. 1 ¶ 2)—provided that adequate data privacy can be guaranteed. The act of crossing national borders should not curtail the data subject's rights, and under no circumstances should it trigger a "race to the bottom" in privacy standards. Under EU DPD Art. 4 ¶¶ 1(a), 1(b), the applicability of national law is a function of the Member State where the data-processing establishment is located.

[3] Translator's Note: An English version of the EU DPD can be found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

In cross-border cloud computing, there is no guarantee that data privacy is regulated at all in the states where the data are actually processed. If the computers used to process the data are offshore, and not on any national territory, protection of personal rights[4] is sure to be nonexistent.

In cases where the data-processing entity has no establishment in the EU/EEA, BDSG § 1(5) sentence 3 provides for designation of a *representative located in Germany*, against which applicable national data privacy law can be enforced.

5. Responsibility

In cloud computing, responsibility for actual data processing and for any violation of personal rights threatens to vanish in the cross-border fog—and this makes it essential to clarify responsibilities carefully in order to evaluate cloud applications under data privacy law. The starting point is the concept of "*data controller*" under BDSG § 3(7) and EU DPD Art. 2(d). The BDSG defines the data controller as "any person or body which … processes … personal data on his, her or its own behalf or which commissions others to do the same," and EU DPD Art. 2(d) sentence 1 assigns responsibility to the person or entity that "determines the purposes and means of the processing." In cloud computing, this begins with the cloud user, which makes the decision to use the cloud and feeds the data into it. Under BDSG § 3(7), responsibility is not limited to the data controller's actual sphere of influence, but extends to contract data processing as well. And BDSG § 11(1) sentence 1 establishes that, when data are processed under contract, the principal is responsible for compliance with data privacy requirements. This means that an entity cannot evade its responsibility by contracting with or working through third parties—though it is possible for the third parties to incur additional responsibilities in the process.

The *data controller is responsible primarily for* ensuring that the processing is allowed under substantive law, which can have implications under administrative, civil and criminal law. The data controller is the designated recipient for: directives from the supervisory authorities under BDSG § 38; claims made by data subjects under civil law, *e.g.*, for information, deletion or correction of data, or for damages; and criminal or administrative penalties (*e.g.*, under BDSG §§ 43, 44).

6. The boundary between "function transfer" and contract data processing

Under EU DPD Art. 17 ¶ 2, Member States shall provide "that the data controller must, *where processing is carried out on his behalf*, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures." German standards for contract data processing are set out in BDSG § 11.

The criteria for contract data processing are not met when a recipient is a third party, which BDSG § 3(8) sentence 2 defines as any person or body outside Germany or *outside a member state of the European Union* (EU) or any other state that is party to the Agreement on the European Economic Area (EEA). In this case, the preferential treatment afforded to data processing under BDSG § 11 cannot be claimed, and the statutory requirements for data transfer (BDSG § 3(4)3) must be met instead. Here the legislature presupposes that the type of transfer arrangement typical of cloud

[4] Translator's Note: We have used "personal rights" as the most meaningful translation for *Persönlichkeitsrecht* in this context.

computing poses special risks for personal rights, because it is impossible for the data controller, the data subject, or national supervisory authorities to adequately monitor the data processing.

6.1 Contract data processing

Technically, cloud computing is *classic contract data processing* as regulated under BDSG § 11. The principal, *i.e.*, the cloud user, should have sole discretion in determining the methods of data processing. Cloud and resource providers are limited to help and support functions and—ideally—are completely dependent on the data controller's instructions. The principal remains responsible for ensuring the confidentiality and integrity of the data, and it generally cannot fulfill this responsibility based on existing cloud structures, since cloud service providers cannot give users any information on the method or location of the data processing services or on security measures. By contrast, data processing in the cloud could conceivably comply with data privacy law if the cloud user, in its role as data controller, were granted total transparency as to basic data processing conditions and available options.

In the classic scenario for contract data processing, the principal must ensure that the agent complies fully with all technical and organizational measures and with substantive guidelines—but the resulting expense is precisely what the data controller seeks to avoid in using the cloud. This *avoidance of oversight and instruction* is only acceptable under two courses of action: 1. the agent makes a binding declaration in the form of a comprehensive, self-imposed commitment; and 2. responsibility for ensuring that these duties are fulfilled is transferred to a competent, independent data controller. This requirement could be met if all providers were to submit to certain external audits or certifications.

6.2 Function transfer

The requirements for function transfer are more demanding. Data privacy laws assume that responsibility for additional processing lies with the recipient of the transferred data, but cloud and resource providers cannot guarantee this: under the ideal cloud computing scenario, they do not and should not know anything about the actual data processing. Cloud *users*, however, must meet the transfer requirements for each unit of data.

To meet these requirements, there must first be a contractual or other justified interest in transferring data to the cloud, and the transfer must be necessary (BDSG § 28(1) sentence 1 nos. 1 and 2). If there is a contractual relationship between the cloud user and the data subject, it can include cloud-based processing. If this is not explicitly provided for, use of the cloud must be "necessary." Though cloud-based transfers may have met the earlier standard of "usefulness[5]," they have been non-compliant at least since September 1, 2009, when the necessity standard came into effect. There are simply no compelling grounds for using clouds that process data outside the EU/EEA, since it can hardly be denied that an adequate supply of cloud services exists inside Europe. The mere fact that cloud services involving providers outside the EU/EEA may be somewhat less expensive is not adequate to meet the necessity standard as defined in BDSG § 28.

[5] Translator's Note: The German term is *Dienlichkeit*.

If there is no contractual relationship between the cloud user and the data subject, the cloud user must be able to prove a justified interest to make function transfer legitimate. Once again, it is doubtful whether cost savings alone constitute a justified interest for the user, though this may be the case when the savings are substantial.

In addition, the data subject has legitimate interests that must be adequately protected (BDSG § 28(1) sentence 1 no. 2). This can be achieved by taking the steps defined in BDSG § 11, but these requirements merely safeguard the data subject's interests: they do not constitute adequate compensation if the cloud user delegates legal responsibility when functions are transferred. That requires the recipient of the transfer to make an additional commitment that offsets the shift in legal responsibility for data privacy from the cloud user to the cloud and resource providers. The parties can accomplish this by agreeing upon severe contractual penalties if the data processing does not comply with instructions—especially if it is improper—and by granting decision-making, oversight and data subject rights that are broader than those for basic contract data processing.

In addition to these requirements, which are generally applicable to data transfers, cloud *transfers to third-party countries, i.e.,* outside the EU/EEA, must meet the conditions set out in BDSG §§ 4b, 4c.

7. Problem: Third-party access

7.1 Legal third-party access

Shifting the data processing location to another country means that third parties in that country—other than cloud or resource providers—may be able to access the data in fact, and may even be authorized to do so by law. This is especially true for *"internal security" authorities, i.e.*, police, other law enforcement authorities, national secret services, and financial authorities. It is even possible for national laws to allow access by private third parties, in some cases because these laws contain no data privacy restrictions at all. The lower the data privacy standard in the country where the data are actually processed, the more cloud-based processing threatens the data subject's interests. The motivation for this type of legal access is not necessarily limited to preventing threats or investigating criminal activity: in many countries, economic espionage in the domestic interest falls under the legal mission and authority of the national secret service. This can never be in the interest of the cloud user, and should not be in the interest of cloud and resource providers, but it is impossible to prevent by law and very difficult to prevent in practice.

While security services are the classic example, other public-sector requesters of cloud data may include *financial authorities*, which may try to access bank data for information on tax evasion or tax fraud, to cite one example. Demand can also come from residency, asylum and immigration authorities, which can use clouds to gather highly relevant information from applicants' countries of origin.

De facto and *de jure* access become particularly problematic when data are processed in a country that not only cannot ensure adequate data privacy, but knowingly and selectively ignores human rights and withholds legal protections, persecuting targeted individuals on political, ethnic, religious, economic or other grounds. In *dictatorships* like Iran or China, government access to cloud computers via governmental or semi-governmental institutions may produce information that can be used as a basis for heightened surveillance, persecution, imprisonment and even execution.

In some circumstances, lawful access to cloud data can be prevented by *technical measures*. Aliasing can prevent data analysis if the data requester has no access to the decoding information. The same is true when the data are encrypted, provided that there is no possibility of decryption, and when the data are processed in virtual spaces to which the requester has no *de facto* read access.

We should bear in mind that many countries have statutes allowing the threat of government-imposed sanctions to be used to compel data processors (in this case the cloud and resource providers) either to completely abandon protections against unauthorized access or to lift them when the authorities demand it. Even Western democracies have statutes *requiring surrender of data decryption keys* when required by the authorities. We should also bear in mind that government entities in nearly every country have the authority to defeat technological security measures, particularly where security is concerned.

7.2 Illegal cloud access

Depending on which security precautions are chosen and implemented, there is also the risk that *unauthorized third parties* will attack the data processed by the cloud user. While the data controller is master of its fate where IT security for its own processing is concerned, it routinely loses all control over security measures in cloud computing. Data security is a routine component of service options.

All of the data privacy goals that the technical and organizational measures are designed to achieve—confidentiality, integrity, availability, transparency for authorized parties, revision-proofing, and unlinkability—*could conceivably be compromised* for cloud-processed data.

Cloud computing also presents a special risk because it offers entirely new *attack strategies for cybercriminals*, who can use the least secure parts of the cloud to penetrate it. Cloud and resource providers are interested solely in making money: they have no vested interest in the data processing itself. As a result, under the right circumstances criminals can easily assume the guise of users and enter undetected to sabotage and/or spy on the data processing.

Technical and organizational measures, as mandated under BDSG § 9 and EU DPD Art. 17 ¶ 1, can limit unauthorized access and even prevent it entirely. It is important to remember, however, that only cloud and resource providers in the EU/EEA countries are legally required to take these kinds of precautions—and even within the EU/EEA, there are often significant gaps in implementation. But while contract provisions cannot prevent legal access to cloud data, cloud users and providers can agree on comprehensive, effective security measures against illegal access.

8. The limits of data privacy oversight

When data privacy violations are committed in clouds outside German territory, there is generally no way to investigate them under German law, either practically or legally. Under the law, the data privacy oversight exercised by supervisory authorities in the German states is limited to the territory of each state. Within the EU and EEA, supervisory authorities can offer administrative assistance to each other, but so far the costs of this option have limited its use to a few isolated cases. While BDSG § 38(1) sentence 1 and EU DPD Art. 28 ¶ 3 provide for routine monitoring without cause, coordinated or joint monitoring is virtually impossible in clouds involving third-party countries—and even within the EU and EEA, where such monitoring is theoretically possible, there are no

actual cases of it. As a result, data controllers that want to *evade data privacy oversight* can use clouds specifically for that purpose. This is particularly true for processing in third-party countries, *i.e.,* outside the EU/EEA, since any monitoring is contingent on contractual monitoring rights granted by the cloud and resource providers. In addition, these rights must be exercised by the cloud user, which generally has no vested interest in data privacy oversight.

Data privacy violations can also constitute *criminal offenses*, allowing for criminal investigation under the German Federal Code of Criminal Procedure (*Strafprozessordnung*, or StPO). Though external data processing can make the investigation process more difficult, the recent addition of § 110(3) to the StPO addresses this problem to some degree by allowing access to external storage media.

9. Minimum requirements for contract data processing

The minimum legal requirement for any cloud application is compliance with the regulations for contract data processing. This is true even for function transfer, since the level of privacy protection afforded to the data subject should not be reduced simply because the data are processed in third-party countries.

The requirements for contract data processing are defined in BDSG § 11(2), effective January 1, 2009. The parties must agree in writing, *i.e.,* in a civil-law contract, to specific terms governing: 1) the subject matter and duration of the contract work; 2) the scope, type and purpose of the processing, the type of data and the category of data subjects; 3) data security measures under BDSG § 9; 4) correction, deletion and blocking of data; 5) the agent's (monitoring) obligations; 6) subcontracting; 7) the principal's monitoring rights; 8) the agent's obligation to provide notice in the event of violations; 9) authority to issue instructions; and 10) deletion of data residing with the agent. Under BDSG § 11(2) sentences 4 and 5, the principal must regularly verify that the processing complies with data security measures and document the results.

Under § 11(2) sentence 1, the agent *must be chosen carefully*, with special attention to the suitability of its technical and organizational measures. This applies not only to the cloud provider as the prime contractor, but also to the resource providers, which act as subcontractors under BDSG § 11(2) no. 6. In addition, BDSG § 11(2) sentence 4 requires the principal to ensure that this requirement is met before processing begins. The cloud user cannot comply unless it knows all of the entities involved in the processing, but in practice it is impossible for the user itself to verify every cloud participant's reliability and data security standards. As a result, users must be able to rely on outside audits—and self-certification does not constitute a reliable audit. At minimum, an independent entity must perform an outside audit and submit a report for the cloud user's review. Because there are so many potential cloud participants, the user must be informed as to which providers are actually processing the data at any given time. Otherwise, the user cannot fulfill its responsibilities as data controller.

It should be self-evident that, in defining technical and organizational measures, the parties must specify *the security procedures that are actually used*, and not merely abstract methods or security goals (BDSG § 11(2) sentence 2 no. 3). This also applies to the monitoring of resource providers that is required of cloud providers under BDSG § 11(2) no. 5. As part of this monitoring, the contract

must require providers to allow—and actually perform—special audits of unusual or improper activities. If the user requests it, it must be possible to actually monitor the processing, *i.e.,* to have access to the relevant data logs.

The contract must also specify requirements and procedures in the event of *unanticipated and/or improper processing*. Under what circumstances must providers proactively inform users of irregularities? Here the parties must consider the rule in BDSG § 42a, which assigns the data controller's obligations to the user: these obligations need to be passed on to the agent.

Practically speaking, the standard operating procedure for cloud applications generally makes it impossible for the user to issue instructions. To compensate, the user must be offered a *range of alternatives*, allowing it to choose specific resources, locations (countries), security levels, and other provider and user options. This is required whenever the actual processing is subject to additional legal requirements, *e.g.,* for data falling under the special categories described in BDSG § 3(9); for data from financial services providers (under § 25a of the German Banking Act, or KWG); for confidential data related to social services (under § 80 of Part X of the German Social Security Code, or SGB); and in special cases involving professional secrecy or official secrets. When sensitive data are processed, they can be labeled to determine how they will be handled in the cloud. This must be covered in the security policies set out in the contract.

The contract must also contain provisions governing the *liability* of the cloud and resource providers towards the user. Cloud-based processing can result in direct injury to the user, and it can injure the personal rights of the affected data subjects, who may be able to bring claims against the user under BDSG § 7 or § 823 of the German Civil Code (the *Bürgerliches Gesetzbuch*, or BGB). Under the liability provisions of the cloud contract, the cloud provider should assume responsibility for all injury for which the user is not responsible. Because the resource providers and the place where injury occurs can be located virtually anywhere, it is strongly recommended that providers and users specify governing law and venue in their contracts.

For longer-term cloud processing, the parties must clarify what will happen to stored data if a *cloud or resource provider becomes insolvent* or is taken over by another company. After processing is complete, the processed data must be deleted. In addition, the parties should think very carefully about what data logs must and may be stored, and for how long. This should also be specified in the contract.

Last but not least, the contract must ensure that there are no obstacles to *data privacy oversight* under BDSG § 38 and that data subjects may exercise their rights (BDSG §§ 33 *et seq*.) without restriction if they so choose.

10. Technical and organizational solutions

The technical and organizational data security measures required by BDSG § 9 and EU DPD Art. 17 ¶ 1 must be disclosed to the user, and under BDSG § 11(2) sentence 2 no. 3 these measures must be expressly set out in the contract. In short, the parties cannot simply rely on the principle of "*security by obscurity*," as is often the case today. Symptomatic of this state of affairs is the way Kai Gutzeit, head of Google's cloud services in Central and Northern Europe, describes his company's approach to data security. Security is primarily a question of trust, he says, much as we trust credit cards and banks today. But if anyone ever did break into Google's top-secret computer

center, he adds, the intruder would find "absolutely nothing" usable, only "meaningless bits and bytes" because Google uses a proprietary file system.

What we need instead is "*security by transparency*," with state-of-the-art security measures. An exhaustive review of the necessary technical and organizational precautions is impossible in this legal analysis, but it is critical for the technical measures to restrict access to the processed data to authorized parties designated by the user—with the possible exception of administrative rights. This could be achieved with a multi-level access regime, encryption capabilities and possibly aliasing tools.

In cloud computing, multiple users work on the same computers and platforms—a practice that presents risks unless stored data are adequately separated. To ensure *compartmentalization of individual contract relationships*, the cloud contract must clearly specify the methods used to separate data from different principals. If this is achieved with encryption, tests must be run to ensure that the system offers adequate security and cannot be easily compromised by other users or by the provider itself.

The user must be given access to the abovementioned range of options via a convenient interface, along with the support required to implement *user-driven application security*.

Both the cloud provider and the entire cloud network must implement a *documented data privacy management system*, to include IT security management and an event management system. We have already discussed the need for transparent audits by an independent entity. Unfortunately, however, the laws regulating this type of audit remain extremely limited, *e.g.,* §§ 4(2), 43(2) of the Schleswig-Holstein State Data Protection Act (the *Landesdatenschutzgesetz Schleswig-Holstein*, or LDSG SH), and BDSG § 9a has yet to be implemented.

11. Clouds outside Europe

If we include entities outside the European Union, the data transfer that is inevitable with cloud computing—and which has *no legitimacy under data privacy law*—makes clouds inherently impermissible.

That said, a broad, free flow of data into countries outside the EU/EEA is theoretically possible, provided the third-party countries offer an *adequate level of data privacy* (BDSG § 4b(2), 4b(3)). The European Commission has determined this to be the case for certain countries, such as Switzerland, Canada and Argentina, but the determination that data privacy is adequate in a non-European country does not mean that entities there can be legally treated as agents under BDSG § 11. They remain third parties, and consequently any disclosure of data is characterized as a transfer.

Because cloud-based data processing cannot meet the necessity standard for transfers under BDSG § 28, and in any case must be treated as contract data processing, clouds with providers outside Europe remain impermissible under data privacy law. This is why some cloud providers give users the option of having their data processed *exclusively within the EU/EEA countries*.

The only way to avoid this conclusion is to assume that the law contains an unintended loophole and apply the rules for contract data processing by analogy. In its decision of December 27, 2001, the European Commission established special standard contract clauses for awarding contracts in third-party countries; these clauses are intended to ensure that agents provide adequate guarantees as

required by EU DPD Art. 26 ¶ 2. This means that, in addition to entering into a *standard EU contract*, the parties must fully comply with the binding requirements of BDSG § 11.

In any case, US companies cannot achieve the data privacy level required under EU standards simply by self-certifying to the *Safe Harbor* list. Cloud contracts based on Safe Harbor benchmarks are also inadequate. These benchmarks helped create a workable bridge between Europe's rigorous data privacy rules and data privacy in the US, which in many respects is non-existent. But even though Safe Harbor was intended as a practical solution for necessary and inevitable data transfers between the US and Europe, it cannot under any circumstances be used to circumvent Europe's more rigorous data privacy rules—as would be the case with cloud computing.

To prove their trustworthiness, US-based cloud providers like Google and Salesforce advertise themselves as holding *SAS 70 Type II audit certification*, which theoretically means that their data centers have been inspected by independent third parties. But this does not entirely satisfy the requirements for contract data processing because—to take one example—it does not address the data subject's substantive and procedural interests in transfers.

Another possibility for cloud participants is to adopt *binding corporate rules* (BCRs), which theoretically gives these companies contractual means for reaching an adequate privacy level as defined by EU DPD Art. 26 ¶ 2 and BDSG § 4c(2). Originally developed for international data processing within corporate groups, this set of legal instruments is now being extended to cloud and resource providers. Under the recommendations of the EU's Article 29 Data Protection Working Party, the BCRs must require the head office, or a member company designated by the group, to take responsibility for violations by any of the group's companies outside the EU. In addition, the BCRs must be approved by the relevant data privacy authorities.

12. Status of the debate

Clouds are offered on the global market and are used both by German companies and by private users to process personal data. Nearly all such data processing takes place out of sight of data subjects, supervisory authorities and the public. Apart from what appears in advertising and technical publications, nothing is known about how clouds actually operate—but that is no evidence that they do not violate data privacy and personal rights. For the present, none of the direct participants (users, cloud providers or resource providers) have any interest in allowing violations to become known. Based on publicly available information and the state of the law, we must assume that violations of data privacy law are inherent in many cloud applications and in fact are being committed on a massive scale.

There is no evidence that *public entities* in Germany are using cloud applications—yet. But we do know that even public entities are considering and testing these options in response to cost-cutting pressures. Large corporations have clearly limited themselves to private clouds, or at least to carefully selected ones, both because of the internal resources at their disposal and in the interest of protecting their own data. For now, the primary user pool for commercial cloud computing probably consists of small and medium-sized business with limited computing capacity and limited legal and technical expertise.

Providers are conscious of the need for confidentiality and integrity, but only for purposes of *market positioning*, and not to protect constitutional rights or because they need to comply with data privacy law. Cloud computing is yet another illustration of the principle that the market begins by doing what is practical, *i.e.*, what is technically and economically feasible and seems to make sense. Only public outcry and government oversight can spur tighter focus on legal requirements. This is clear from legal publications, which so far have adopted the premise that it is pointless to fight reality, either claiming that the law has adapted to the *status quo* or arguing that it should—and in the process downplaying the consequences for personal rights or ignoring them altogether.

13. Next steps

Action at the international level has produced the US-dominated Cloud Security Alliance (CSA), which seeks to develop guidelines for secure cloud computing. Following the recent launch of **EuroCloud Deutschland_eco***, the German cloud computing industry now has an association* that is part of the EU's EuroCloud Network. EuroCloud Deutschland_eco's goals include increasing transparency for users, introducing a seal of approval, clarifying legal issues, fostering dialog between providers and users, and cultivating cloud computing expertise.

When viewed as digital protection of constitutional and human rights, data privacy is neither discrimination against cloud providers in specific countries, nor a source of market distortion, nor an obstacle to technology, but rather a *cloud enabler*. In fact, professional use of these systems is irresponsible without the necessary level of privacy protection.

With *international regulations* in place, it would doubtless be possible to make cloud-based data processing independent of location, and to mandate that cloud-based data processing be governed exclusively by the law that applies to the user or to the cloud provider in direct contractual relationship with the user. So far, however, there is no evidence of efforts in this direction. Given the inconsistency—and in some cases the inadequacy or total absence—of national laws on data processing in general and data privacy in particular, it is unrealistic to expect international standards for the moment. As a result, we have no alternative but to implement a clear system of legal protections that begins with the data controller, *i.e.*, the cloud user.

The first step toward this goal is an *objective review*. Market transparency itself, along with transparency of the cloud-based data processing methods currently on the market, can clean up the market to a certain degree, and it is the indispensable prerequisite for a public discussion involving all stakeholders. These include not only users and providers, but supervisory authorities, IT professionals (especially security technology researchers), consumer advocates, and naturally members of the public and the political class.

Researchers, the business community and supervisory authorities face the challenge of working with the appropriate organizations to devise *protection profiles* for clouds and to develop and establish audit procedures. One first step towards international regulation would be to develop specific standard contract clauses and/or binding corporate rules (see Section 11 above).

The core principle of the "free cloud," which still has currency today, cannot meet the demands of modern data privacy. It can only be viewed as a game or experimental application with the potential to generate *trusted and trustworthy clouds* with integrated data privacy and data security guarantees. If

these trustworthy clouds are not made available to the market, the fundamental principle of cloud computing cannot survive—at least not for any data that are worth protecting.