October 2017

Issue Brief # 2017 - 04

Cloud Security: Challenges and Solutions in the Context of the European Union

Adam Palmer
Financial Services Roundtable (BITS)

Thomas Rickert
Rickert Rechtsanwaltsgesellschaft mbH

Jan Schlepper
Rickert Rechtsanwaltsgesellschaft mbH

Center for Cyber & Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Cloud Security: An Overview of Challenges and Solutions in the Context of the European Union

With widespread adoption of cloud based infrastructure, new security and privacy concerns have increased. In the European Union (EU), there are significant concerns about the inherent risks of placing sensitive data on a third party, (often) US company controlled, cloud infrastructure. This article examines the key compliance concerns for cloud adoption in the EU and proposes a basic checklist for managing the security and compliance issues within the cloud.

Rather than increasing risk, cloud based systems actually improve security and scalability. Cloud systems provide many other operational benefits that allow for low cost, secure, and scalable data storage. This article will also address some of the regulatory issues of layering third party security services on top of cloud infrastructure.

Cloud providers are improving support for compliance and security; however, these providers still need to confirm that their solutions meet the requirements of heavily regulated industries such as the financial services sector.

In Europe, numerous data privacy and security laws apply to cloud infrastructure. This article will focus on EU compliance with the General Data Protection Regulation (GDPR) and also highlight Germany as an example of a large European market approach to cloud regulations.

EU Cloud Regulation and Cybersecurity

With the General Data Protection Regulation (GDPR) becoming effective in May 2018, it is important for companies to develop and implement a strong data protection program for cloud services in the EU.

The GDPR applies when:

a) either the (cloud) service provider or the customer has a place of business in the European Union; and

b) personal data is being processed. Note that the GDPR is not location dependent. It applies if any location is processing personal EU data.

GDPR is also applicable when personal data of an individual is processed, if that person is a resident of the European Union. Permanent resident status is not required—this can apply to any person who is a temporary resident or who lacks an official legal visa status, but resides in the EU. GDPR also applies if products or services are offered to such individuals or if behavior is tracked within the cloud service.

The main responsibility for GDPR compliance lies with the data controller, but the processor also bears significant responsibility. Typically, cloud services to customers are based on a data processing agreement by which providers process the data on behalf of data controllers. GDPR now holds both parties responsible for the compliance with data protection regulations (not only the data controller).

A data processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." This definition in Art. 4 No.8 GDPR does not reference the responsibilities of the parties or the processor being bound by instructions from the controller. This illustrates a basic goal of GDPR to strengthen the processor's own personal responsibility. However, this does not mean that the controller is no longer responsible for the compliance of data processes. Art. 28 GDPR states that the controller must use a processor "providing sufficient guarantees to implement technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

In addition, the data controller has control rights regarding the compliance by the processor and is required to control and document this compliance. This also reflects the new direction of the GDPR to have both the data controller and processor responsible for the data processing.

The GDPR requires compliance by the data processor with the requirements for *state of the art technical and organizational measures* that can be proven with corresponding certificates. The types of certification that will be accepted by cloud clients as being acceptable and trustworthy are still to be determined. It is therefore strongly recommended for cloud services providers to develop a strong and comprehensive record of the technical measures taken to secure the customer´s data. Even if a cloud security provider is layered on top of the provider, such as the

AWS cloud infrastructure, the security provider still also has responsibility to implement all necessary security measures as a data processor.

Documentation of Compliance

Data processors must maintain a record of processing activities relating to the controller´s data. Such a record must also be provided to EU authorities upon request. A record of processing activities should be developed and kept up to date for every customer for whom services are provided.

The data processor may only use sub-processors with prior consent from the customer. This includes any technical service provider that will have access to any personal data from the data controller. Also, the sub-processor must sufficiently guarantee compliance with GDPR technical and organizational measures.
The GDPR now explicitly clarifies that the processor is liable for the compliance of sub-processors. Therefore, it is important for controllers to review and control sub-processor actions to ensure compliance and proper controls. An internal policy to ensure continuing control and surveillance of sub-processor compliance should be implemented.

Transfer of Data to Countries Outside the EU

The GDPR explicitly states that the data processor is responsible for compliance with additional requirements for a transfer of data to non-EU countries. Even though there are several methodologies to make a transfer to non-EU countries, all of these methods face significant political criticism and skepticism within the EU. Trust can be increased if data is processed only within the EU.

Privacy by Design and Privacy by Default

Art. 25 of the GDPR implements two new principles: privacy by design and privacy by default. Both of these principles require the responsible data controller to take data protection principles into account when designing and configuring their systems of data processing.

To support customers in fulfilling their GDPR obligations, it is imperative that cloud systems are designed to ensure compliance with data protection. Cloud systems need to be designed to comply with the EU basic data protection principles, in particular with the principle of data minimization. EU cloud customers also need the possibility to set the default of their cloud systems in a way that data protection requirements are easily met. This will primarily relate to data minimization as well

as the requirement to restrict access to personal data of those persons who need access to fulfill their tasks based on the purpose for which the data was collected.

Remedies and Sanctions

Under GDPR, the data subject can now make claims against both the data processor and the data controller. This includes seeking compensation for damages, and is not restricted to damages that derive only from the violation of an obligation by the processor. A violation of the obligation to report processing activities can result in a fine of up to 10,000,000 EUR or 2 % worldwide annual turnover.

As GDPR increases the data processor's responsibility, the cloud service providers also need to review their data protection policies, processes and technical or organizational measures for compliance with GDPR requirements. All data processes should be documented so compliance can easily be proven to data subjects and authorities.

Processes must be developed and implemented before 25 May 2018 for GDPR compliance.

Cloud Cybersecurity Regulation in Germany: An EU Regulatory Example

Using Germany as an example, the use of cloud IT systems and IT cloud based security infrastructure is subject to the provisions of the German Federal Data Protection Act ("BDSG"). The BDSG protects the privacy rights of individuals whose personal data is collected, processed or used. The data itself is *not* protected; but rather, the rights of the individuals who the data applies to is what is protected. This right is part of the fundamental right to *informational self-determination* provided by German law and generally recognized across the EU.

The BDSG does not cover processing of all data, but only of so-called "person-related" data. This is defined in section 2 para. 1 BDSG as: "Person-related data is individual information on personal or material circumstances of a specific or identifiable individual (person affected)." This includes for example the name, address, date of birth, email address and private email content, the phone number and account data.

The BDSG also defines so-called "Special categories of personal data". This covers all information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life. The BDSG defines

strict requirements for the processing and dissemination of such data. The BDSG establishes a prohibition on processing person-related data subject to consent. This means that processing data is generally prohibited, but is allowed under certain circumstances.

The BDSG lists only two instances in which data processing is allowable:

(1) If the subject has consented. Consent by the subject to data processing is subject to certain conditions for legalisation of data processing. Consent must precede data processing, be voluntary, with knowledge of the exact circumstances of data processing, and be given explicitly.
(2) If permitted by the Act or any other legal provision. If permitted by another legal provision, the following regulations cover this data processing:
    - Section 28 BDSG (commercial purposes). Section 28 para. 1 no. 2 BDSG permits processing of person-related data to safeguard justified interests of the responsible body and the data subject has no overriding interest in exclusion from processing. At this point the interests of the responsible body must always be weighed against the right of informational self-determination of the persons affected. *Under these provisions the justified interests of the responsible body can also arise out of the interest of protecting the IT system and data security.*
    - Section 13 BDSG (public bodies). Under section 13 para. 1 BDSG, data processing is permissible if required to perform the functions of public bodies*. This can also cover protection of the bodies' IT systems and data.*

A cloud provider or client of such a provider is accordingly required to take all reasonable measures necessary to ensure data security, including protecting the IT system and infrastructure with security hardware and software, such as third party security solutions, if the existing cloud infrastructure is inadequate.

It should also be noted that the annex to section 9 BDSG includes a catalogue of measures which a responsible body must follow at all times, including access control, as stated in section 9 subsection 3 BDSG. The responsible body must ensure that individuals with access to person-related data can only access the data that they need to perform their tasks. Configuration of access and authorization rights must accordingly ensure that nobody has access to data and IT areas that go beyond their authorization.

Principles of Cloud Data Protection

The German data protection laws should always be viewed in the context of the general EU principles of data reduction, data economy, and restricted use. Principles of data reduction and data economy are stated explicitly in the BDSG. In accordance with these principles, all collection, processing and use of person-related data and the design and choice of data processing systems must always have the aim of collecting, processing and using as little personal data as possible. This also means that data must be deleted as soon as it is no longer required for the specific purpose it was authorized for storage.

Data Transfer within a Cloud Infrastructure

The Challenge: Transfer of personal data to other EU member states is possible without difficulty due to the uniform data protection provisions in the European Union. By contrast, the BDSG has special provisions for data transfer outside the EU.

Transfer of personal data to foreign bodies is prohibited if the data subject has a legitimate interest in excluding transfer, specifically if the foreign body in question does not have an adequate level of data protection. (See section 4b para. 2 sentence 2 BDSG). In practice, this means that data transfer to non-EU member states is only possible if an adequate level of data protection (i.e. comparable to the regulations prevailing in the EU) is ensured. In addition to checking the permissibility of data transfer generally (in accordance with sections 28-30a BDSG), data transfer abroad also requires checking the permissibility of transfer to non-EU nations (two-stage check). Section 4b BDSG also contains additional requirements for the transfer abroad of person-related data which go beyond the general requirements of the BDSG for storage and processing of data. In accordance with section 4b para. 2 BDSG transfer to countries outside the European Union may only take place if the body abroad receiving the data has an adequate level of data protection.

The Solution—EU Model Contractual Clauses : Companies with a business location in the United States do not have an adequate level of data protection, in principle, under EU law. To establish the necessary, adequate level of data protection for US companies and protect client data, there is the possibility of adopting the so-called "EU Model Contractual Clauses" into contractual agreements. These are standardized contractual provisions, which have been developed by the EU Commission based on Art. 26 subsection 4 of the EU Data Protection Directive. Through the utilization of the EU Model Contractual Clauses, guarantees for the protection of privacy are created, which allow a *certificate of exemption* for the export of data.

If contractual clauses are used with identical wording to EU Model Contractual Clauses, then no approval procedure by EU authorities is required for data transfer from the EU to the United States. The transfer of data to subcontractors of the contractor in a third country is also possible to the extent that the written consent of the principal has been collected in advance; and, in relation to the subcontractor, the EU Model Contractual Clauses are also binding.

Employee Data Protection: A Unique EU Emphasis and Challenge

German data protection law and the telecommunications law require special handling of the personal data of a company's employees. IT security technology must take into account these employee rights in accordance with the statutory requirements of each individual employee in terms of their personal data.

Again using Germany as an example, confidentiality of employee data is regulated in section 88 of the German Telecommunications Act (TKG):

> *"(1) The content of telecommunications and the detailed circumstances thereof, in particular the fact of whether a person is or has been involved in telecommunications traffic, shall be subject to telecommunications confidentiality.*
>
> *(2) Anyone providing telecommunications services is obliged to maintain telecommunications confidentiality."*

In accordance with section 3(6) TKG, a service provider is: "… anyone wholly or partly commercially (a) providing telecommunications services or (b) involved in providing such services."

Heuristic (Signatureless) Based IT Security Technologies

Signature (or heuristic), suspicion-based IT security technologies may operate at various points in the IT infrastructure and examine incoming and outgoing data traffic or patterns of behavior for indicators which are suspicious. If a suspicious element is identified, it is generally blocked, extracted, and subjected to closer examination, so that there is no extensive storage and processing of data. However, by their nature, these checks can, in rare circumstances, result in legally significant processing of personal data of innocent employees (false positives).

The storage and transfer of what might ultimately be an "innocent" file, that contains personal data of an employee, might constitute a violation of the German telecommunications confidentiality law provisions. However, German law allows

the employer to obtain knowledge of the content of communications on an IT system if this is necessary to protect the company's technical systems. A judgment of such a need requires consideration of each specific case. Review of personal data for security reasons should be reduced to the minimum possible extent (principle of data economy). This can be achieved by using a cloud based security technology that drastically reduces—to the point of nearly eliminating—false positives.

The New German IT Security Act

The German IT Security Act, which has now entered into effect in Germany, is designed to support a new level of IT security in Germany, particularly among the operators of critical infrastructure. The Act creates a series of new, unfamiliar and complex, obligations for the companies affected, and indirectly also creates new requirements for operators of IT cloud infrastructure.

New requirements include record keeping compliance with these new requirements through security audits, establishing and maintaining procedures for reporting IT security incidents to the responsible German Federal Office for Information Security (BSI), and operating a contact office for all questions relating to IT security.

It has not been determined how these new requirements for IT security measures will be fully implemented, but there are indications that the Act will be aligned with the requirements of the ISO 27001 series.

For the energy sector, German authorities have created a draft security "catalogue" of services and requirments developed by the German Federal Network Agency. It is expected that a comparable approach will be taken for the other sectors. This catalogue includes requirements for protections against threats to telecommunication and IT systems that should be achieved specifically by choosing suitable, appropriate, and "state of the art" IT security measures which:

i. ensure availability of the systems and data to be protected,
ii. ensure the integrity of the information and systems processed, and
iii. ensure confidentiality of the information processed on the systems in question.

The preceding section suggests that simply implementing basic measures, such as the use of antivirus software, firewalls, etc., is inadequate for the purposes of ensuring an appropriate level of security for IT systems. Instead, achieving the desired level of state of the art protection requires a holistic approach that is continuously reviewed for its efficiency and efficacy. This is exactly how cloud

based advanced cybersecurity infrastructure, with its innovative and state of the art approach to evolving threats, is relevant. Rather than being a concern, cloud based infrastructure, along with third party layered security solutions, may actually be a necessary holistic approach to compliance.

German companies covered by the IT Security Act are obliged by statute to certify every two years that the requirements for state of the art security are met. Again, cloud based security technologies, that continuously develop and improve in response to potential threats, provide the EU companies involved with all the information they need to demonstrate compliance with the statutory security requirements. A cloud infrastructure provider also has the capability to assist clients to report to the BSI in the event of an incident.

Implementing Security Services in the Cloud

Processing of personal data in Germany is authorized if it is necessary to protect legitimate interests of the responsible body and the person affected does not have an overriding interest in excluding their data from processing. The BDSG defines a justified interest specifically in section 9, which requires both public and private bodies to take such technical measures as are required to ensure the protection of the data they process. This includes the use of suitable IT security technology.

However, section 31 BDSG, requires that personal data be stored *exclusively* for purposes of data protection or data security, or to ensure the proper operation of a data processing system. Personal data processing for security may only be used for these purposes.

Finally, it is necessary to consider whether the interest of the responsible body (i.e. the processing company) in processing personal data (in a specific volume and specific manner) is outweighed by the interest of the affected person in excluding their data from processing. This consideration also involves the principle of data economy, which states that personal data may only be processed to the extent required to satisfy the justified interests of the responsible body, and also that such data may only be stored for such time as the justified interests require.

Generally, if implementing security products or cloud based systems supports an entity's interest in protecting its infrastructure against attacks, this will outweigh the interest of persons in protecting their personal data from processing.

Conclusion

Cloud based systems are really not a new paradigm, but rather a new platform that simply requires additional attention to enforcement of privacy controls. Industry groups have outsourced security operations and data storage to third parties for many years. These third parties are typically managed through contractual compliance and controls that assure a third party will provide adequate security. Cloud applications are simply another vendor application for outsourced data processing and security. However, the cloud customer must be comfortable with internal security controls and confident these controls can be adequately extended and protected outside the enterprise network walls.

Cloud services offer many advantages that may actually make compliance with EU compliance controls easier. Some controls that may offer benefits for security and compliance include:

- Controls for limiting where data will be stored in cloud based systems.
- Contractual assurance of adequate GDPR and EU security controls and record keeping by cloud provider to evidence controls are implemented adequately.
- Emphasis on collaboration between data processor, controller, and cloud client, on threat information.
- Partnership with law enforcement and private sector where possible to share threat intelligence between public and private sectors.
- Embedded privacy compliance into policies and infrastructure at beginning of cloud operations.
- Although not a total solution, encryption of data by default should be implemented.
- Redundancy and adequate back-up systems are scalable in the cloud.
- Focus on blockchain as a tool to bolster interoperability and better network tracing, for auditing and compliance confirmation, may also be possible.

About the Authors

Adam Palmer (MBA, JD, CISSP, CIPP) is Vice President, Cybersecurity Risk Management, at the Financial Services Roundtable (BITS). He is a former US Navy JAG Prosecutor, and a former Manager of the UN Global Programme Against Cybercrime. His email address is: adamppalmer@gmail.com

Thomas Rickert is a lawyer and managing partner of Rickert Rechtsanwaltsgesellschaft mbH, Bonn, Germany (www.rickert.net). He specializes in all legal aspects relating to digital business, in particular IT law, cybersecurity, IP law and data protection. From 2011 to 2015 he was a member of ICANN´s GNSO Council.

Jan Schlepper is a lawyer based in Bonn, Germany, at Rickert.Net since 2013. A certified Data Protection Officer, he specializes in IT law and data protection law, and is acting as an external Data Protection Officer for several international companies.

About the Center for Cyber and Homeland Security

The Center for Cyber and Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats.