Whitepaper on German Data Protection

February 2017

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document explains how customers can use AWS services in compliance with the German data protection act, called Bundesdatenschutzgesetz (BDSG), and retain control over their content in general, and personal data in particular.

Introduction

This paper will cover the following topics:

- How AWS services operate.
- How customers can comply with the BDSG, address their security needs, encrypt and otherwise protect their content when using AWS.
- How the BDSG relates to AWS services in relation to customer controls and the associated technical and organizational measures.
- Relevant compliance considerations, including how customers can control the geographic regions where their content can be stored and accessed.
- The respective roles the customer and AWS each play in managing and securing content processed with AWS services.

This information should answer questions typically asked by AWS customers as they consider the implications of the BDSG. Customers are responsible for addressing other relevant considerations, such as the customer's need to comply with industry specific requirements and best practices.

Please note that this paper is provided for information only. It is not legal advice, and should not be relied on as legal advice. As each customer's requirements will differ, AWS encourages its customers to obtain appropriate advice on their implementation of privacy and data protection requirements, and more generally, applicable laws relevant to their business. Customers use the AWS services to process a wide variety of "customer content", which includes all types of data, text, audio, video and software. AWS treats all customer content (whether it is personal data or not) with the same high standard that is appropriate for personal data. For this reason, this paper will refer to customer content in general and all references in this document to customer content include personal data (as a potential subset of customer content).

Due to the direct applicability of the General Data Protection Regulation, the BDSG will likely be amended or replaced with a General Data Protection Act. We are tracking such changes and will continue to comply with applicable laws.

Bundesdatenschutzgesetz

Data Processing Under the BDSG

In the context of BDSG, "processing" includes any operation or set of operations performed on personal data (e.g., collection, storage and use of such data). Personal data is defined as information concerning the personal or material circumstances of an identified or identifiable individual (the data subject). In addition, the BDSG makes a distinction between data controllers and data processors:

- **Data Controller (Verantwortliche Stelle oder Auftraggeber)** – the party which collects, processes or uses personal data, or who uses other parties to this on its behalf.
- **Data Processor ("Auftragnehmer")** – a party which processes personal data on behalf of the controller.

The data controller is responsible for ensuring that personal data is processed in compliance with data protection obligations, including verifying that the personal data is being processed fairly and lawfully, and that the data is secured against unauthorised or unlawful processing.

AWS as Processor of Personal Data for the Customer

AWS services are used in many different contexts for different business purposes. Often more parties than merely AWS and the customer may be involved in the data lifecycle of personal information included in customer's content processed using AWS services or any computational results that customers or their users derive from the foregoing through its use of the AWS services. For example, a customer's customers or its affiliates. We will generally refer to customer content in the remainder of this whitepaper. As a general guide, where personal data is processed using the AWS services:

- The customer will be the controller in relation to that personal data if the customer determines the purpose for which the personal data will be processed and has chosen how it will be processed. In this scenario, AWS is the processor.

- The customer will be a processor in relation to that personal data if the customer is merely processing the personal data on the AWS network on behalf of and according to the wishes of a third party (who may be the controller, another third party in the supply chain, or an individual acting in a purely domestic capacity). Here, AWS is the sub-processor.

The Article 29 Working Party has also issued guidance on cloud computing and agrees that generally the cloud provider (i.e. AWS) will be the data processor.

The applicability of these concepts plays a vital role as they determine the responsibility for compliance with data protection rules. As a provider of infrastructure as a service, AWS offers a variety of service features and controls that customers can use in a self-service manner. AWS customers have control over what data they want to "process" on AWS, and where and how to protect it. In particular, AWS customers are empowered to use encryption to protect their content by rendering it unintelligible. AWS does not have visibility into or knowledge of what customers are storing on the AWS network, including whether or not that content includes any personal data.

Data Processing Agreements and Model Clauses

For customers who use the AWS services to process personal data, AWS provides a data processing addendum to help customers meet their data protection obligations. If the customer wishes to transfer personal data from the EU to a country outside the European Economic Area, AWS offers Model Clauses as an Annex to a customer's data processing addendum. Customers can rely on the AWS data processing addendum including the Model Clauses since, on March 6, 2015, the AWS data processing addendum, including the Model Clauses, was approved by the group of EU data protection authorities known as the Article 29 Working Party. For more details on the approval from the Article 29 Working Party, please visit the Luxembourg Data Protection Authority webpage here:

http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html.

Access to Customer Content

AWS does not access or use customer content for any purpose other than to provide the customer and its end users with the selected AWS services. AWS never uses customer content for its own purposes, including marketing or advertising.

AWS provides customers with a number options for encrypting content when using AWS services, including using AWS encryption features, managing their own encryption keys, or using a third-party encryption mechanism of their own choice.

Generally, AWS will not know if customer content contains personal data. As set out above, AWS treats all customer content with the same high standard that is appropriate for personal data. In this way, all customer content benefits from the same robust security measures that protect personal data. AWS simply provides the compute, storage, database and networking services selected by the customer with best-in-class security measures applied to the cloud infrastructure provided by AWS. The customer is then free to build on that infrastructure those security measures that are needed based on the customer's own, unique requirements.

Government Rights of Access

Customers frequently ask about the rights of domestic and foreign government agencies to access content held in cloud services. Customers are often concerned about issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them depending upon where they – or their customers – are doing business. Customers should seek advice to understand the application of relevant laws to their business and operations.

When concerns or questions are raised about the rights of domestic or foreign governments to seek access to content stored in the cloud, it is important to understand that relevant government bodies may have rights to issue requests for such content under laws that already apply to the customer. For example, a company doing business in Country X could be subject to a legal request for

information even if the content is stored in Country Y. Typically, a government agency seeking access to the data of an entity will address any request for information directly to that entity rather than to the cloud provider.

Generally, Member States of the EU have legislation that enables public law enforcement and national security bodies to seek access to information. Foreign law enforcement bodies may also work with the local law enforcement and national security bodies to obtain access to information in the EU. In fact, most countries have processes (including Mutual Legal Assistance Treaties) to enable the transfer of information to other countries in response to appropriate, legal requests for information (e.g. relating to criminal acts). There are certain criteria that must be satisfied under the relevant law before a request for access by the relevant law enforcement body will be authorized. For example, the government agency seeking access will likely need to show it has a valid reason for requiring a party to provide access to content, and may need to obtain a court order or warrant.

AWS Policy on Granting Government Access

AWS is vigilant about protecting our customer's content, regardless of where a request for content comes from or who the customer is. AWS will not disclose customer content unless required to do so to comply with a legally valid and binding order, such as a subpoena or a court order. Non-U.S. governmental or regulatory bodies must typically use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. AWS carefully examines each request to authenticate its accuracy and verify that it complies with applicable law. AWS will challenge requests that are overbroad, exceed the requestor's authority or do not fully comply with applicable law, e.g. in case the data is not stored in the jurisdiction of the requesting authority which as a result of a recent court ruling, has great chances of success. AWS also attempts to re-direct the request directly to the customer, and in doing so may provide the customer's basic contact information. If AWS is compelled to disclose customer content, it notifies customers before disclosure to provide them with the opportunity to seek protection from disclosure, unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. Additional information can be found in our latest transparency report and our Amazon Law Enforcement Guidelines.

AWS Regions: Where Will Content be Stored?

AWS data centres are built in clusters in various countries around the world. We refer to each of our data centre clusters in a given country as a “Region”. Customers have access to sixteen AWS Regions around the globe, including three Regions in the EU – Ireland (Dublin), Germany (Frankfurt) and United Kingdom (London) – with more Regions due to come online through the next year. Customers can choose to use one Region, all Regions or any combination of Regions. The customer's choice is binding for AWS. Figure 1 shows AWS Region locations.

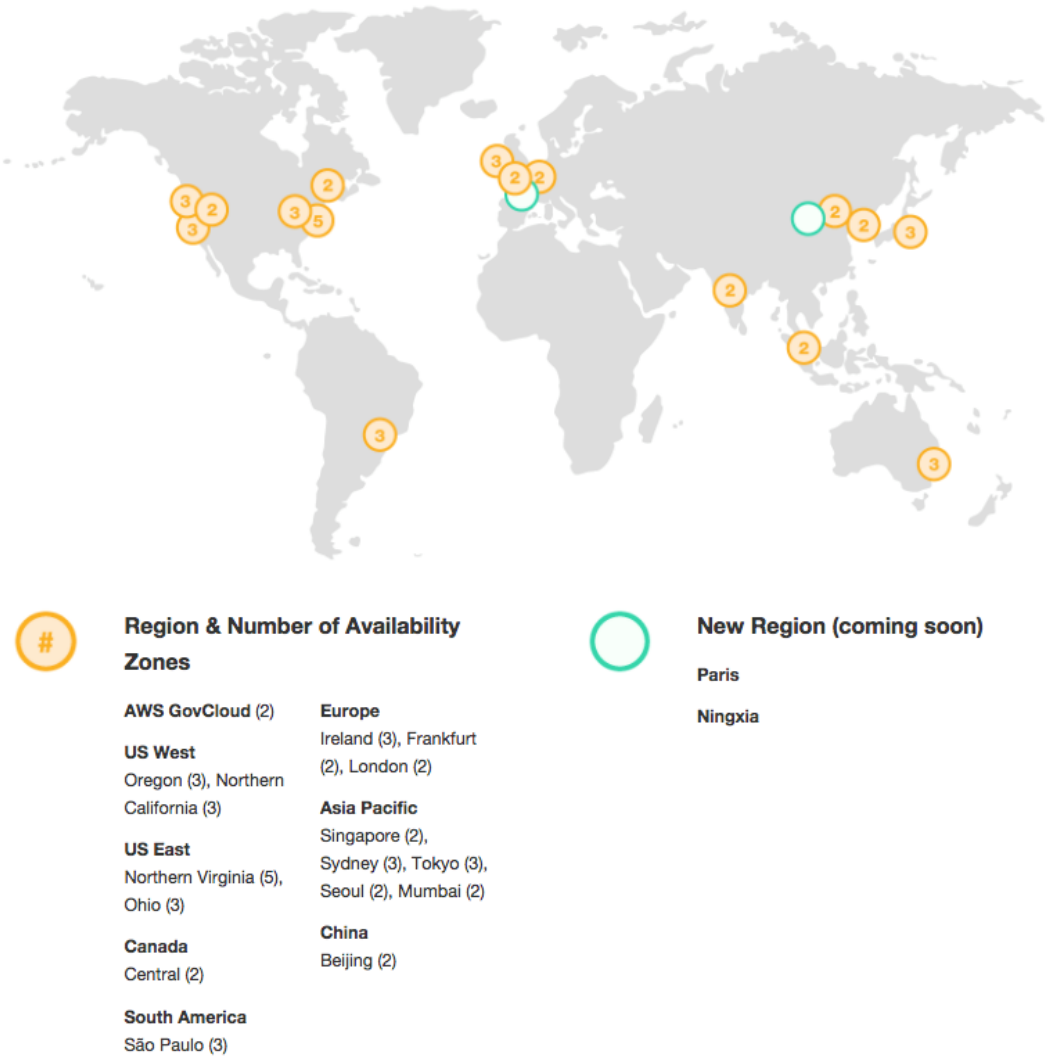


Figure 1 – AWS Regions and Availability Zones

AWS customers choose the AWS Region(s) where their content will be hosted. This allows customers with specific geographic requirements to establish environments in a location(s) of their choice. For example, AWS customers in Europe can choose to deploy their AWS services exclusively in the EU (Frankfurt) Region. If the customer makes this choice, the customer will be able to point to a specific location where their content will be stored in Germany. Unless customer chooses another region, customer content will not be mirrored on servers of another AWS Region.

Customers can replicate and back up content in more than one Region, but AWS does not move or replicate unless otherwise instructed by the customer.

Customers retain control of which Region(s) are used to store and process content. AWS only stores and processes each instance of customer content in such Region(s), and otherwise will not move customer content outside of the customer's chosen Region or Regions, except as legally required.

Selecting Regions

When using the AWS management console, or in placing a request through an AWS Application Programming Interface (API), the customer identifies the particular Region(s) where it wishes to use AWS services. Figure 2: Selecting AWS Global Regions provides an example of when uploading content to an AWS storage service or provisioning compute resources using the AWS management console.

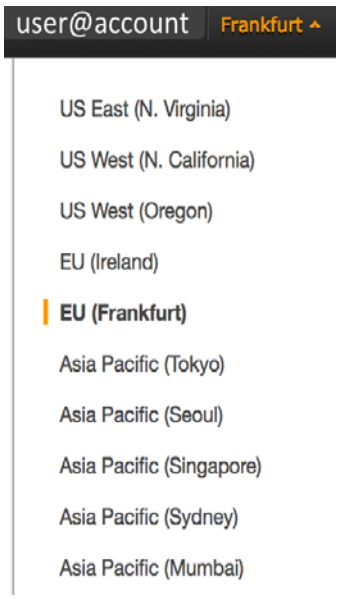


Figure 2 – Selecting AWS Global Regions in the AWS Management Console

Customers can use Virtual Private Cloud (VPC) to define the AWS Region to be used exclusively for their compute resources. Amazon VPC allows customers to provision a logically isolated section of the Amazon Web Services (AWS) cloud where they can launch AWS resources in a virtual network that they define. Using Amazon VPC, customers can define a virtual network topology that closely resembles a traditional network that might operate in their own data centre.

Any compute and other resources launched by the customer into the VPC will be located in the Region designated by the customer.

Security of Customer Content

AWS is responsible for managing the security of the underlying cloud environment. This is called the security of the cloud. The AWS cloud infrastructure is one of the most secure cloud computing environments available.

AWS is vigilant about our customer's security. We have implemented sophisticated technical and physical measures to protect our environment. A complete list of the security controls built into the core AWS cloud infrastructure, platforms and services is available in the following whitepapers:

- Amazon Web Services: Overview of Security Processes
- AWS Risk and Compliance

Comprehensive information can also be found below in in section Technical and organizational measures below.

AWS Operates a Robust Security Incident Management Procedure

An important part of the AWS security controls is what AWS does to detect and respond to identified security risks. AWS utilizes 24x7x365 coverage to detect incidents and to manage their impact and resolution.

AWS defines, administers, and monitors security for the underlying cloud infrastructure (i.e. the hardware, the facilities housing the hardware and the network infrastructure). For example, AWS regularly scans all internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). Once detected, AWS employs industry-standard best practice procedures to drive resolution of business-impacting events.

Because AWS manages the infrastructure and the security controls that apply to it, AWS can do the following:

- Identify potential incidents affecting the infrastructure.

- Determine if any access to customer content resulted from that incident.
- Determine if that access was actually unlawful or unauthorized. For example, access would be unauthorised if it was in breach of AWS' security policies.

If AWS becomes aware of either (a) any unlawful access to any Customer Data stored on AWS equipment or in AWS facilities; or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of customer content (each a "Security Incident"), AWS will notify Customer of the Security Incident. AWS does this regardless of whether the customer content is personal data or not and whether it is sensitive data or not.

AWS' incident management plan is verified and certified under ISO 27001, 27017, 27018 and 9001 and is audited in detail in the AWS Service Organisation Control (SOC) 1, 2 and 3 reports. All procedures and policies such as ISO27001, ISO27018 and SOC 3 are available at https://aws.amazon.com/de/compliance/.

Customer can also report potential vulnerabilities to AWS. The AWS Vulnerability Reporting page describes how AWS' addresses reported vulnerabilities.

Shared Responsibility for Managing Cloud Security

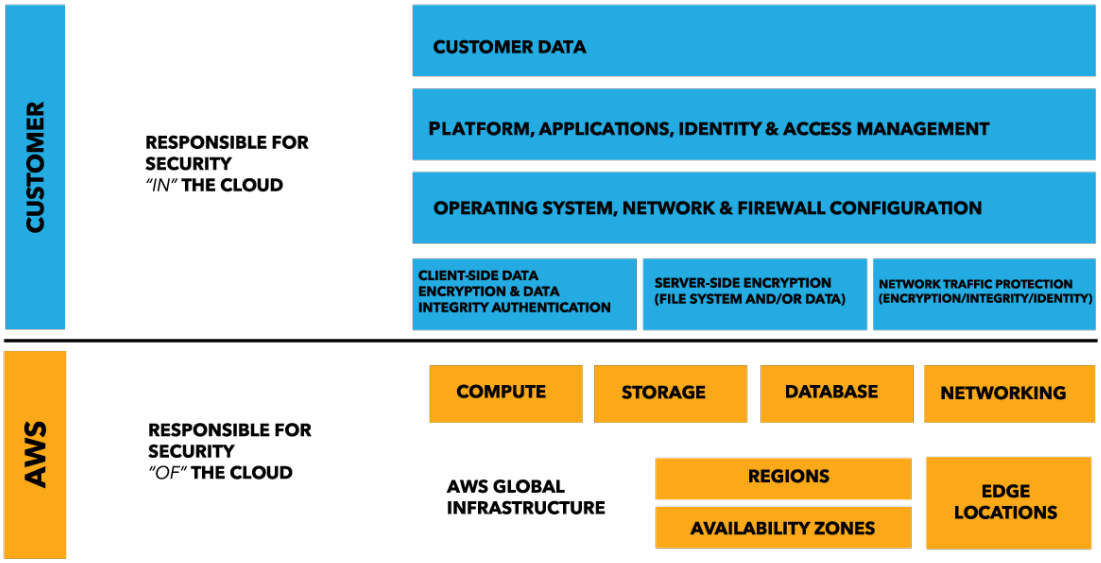
Moving IT infrastructure to a cloud based infrastructure powered by AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have important roles for the operation and management of security in their areas of responsibility. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for managing the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features. The customer will generally connect to the AWS environment through services provided by third parties (for example internet service providers). AWS does not provide these connections and they are therefore part of the customer's area of responsibility. AWS also

does not operate the data processing tasks for the customers. Customer should consider the security of such connections and the security responsibilities of such third parties in relation to their systems. This is really no different from working with a network service provider who brings connectivity to on-premises data centres. The respective roles of the customer and AWS in the shared responsibility model are shown in Figure 3 below.

Figure 3 – Security Model

The Shared Responsibility Model and Customer Content

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:



- Security measures that the cloud service provider (AWS) implements and operates – "security *of* the cloud" related to the security of the physical infrastructure as availability and integrity; and
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – "security *in* the cloud"

While AWS manages security of the cloud, security in the cloud is the responsibility of the customer, because customers retain control of what security measures they choose to implement to protect their own network, systems, platforms, applications, and content (from the server OS level up to the

application level) – no differently than they would for applications in an on-site data centre. As part of its different service offerings, AWS provides its customers with a selection of security measures and our customers can also choose to use a variety of third party security solutions. AWS customers have the complete freedom to design their security architecture to meet their compliance needs to meet their internal and any external legislative / regulatory requirements. This is a key difference to traditional hosting solutions where the provider generally decides on the architecture. AWS enables the customer to decide if security measures will be implemented, and if so, the customer is empowered to decide which security measures to implement in the cloud and determine whether these are appropriate for its business. If, for example, a high availability architecture is required to protect the data, the customer may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to data is required, the AWS controls enable the customer to implement access rights management concepts both on a systems level and through encryption on a data level. AWS therefore provides the customer with direct controls over many elements that form technical and organizational measures in respect to data security.

We are vigilant about the security of our underlying cloud environment, and have implemented sophisticated technical and organizational measures against unauthorized access. As mentioned above, customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001 , 27017 and 27018 certifications and PCI-DSS compliance reports. These reports and certifications are produced by independent third party auditors and attest to the design and operating effectiveness of AWS security controls. The SOC reports are issued twice a year and cover the six-month periods from October 1 to March 31, and April 1 to September 30. The ISO 27001, 27017 and 27018 are annual certifications. PCI-DSS compliance reports are also issued annually.

Customer Controls (Technical and organizational measures) - § 9 BDSG and appendix to § 9 BDSG

The data controller is responsible for implementing appropriate technical and organizational measures to protect the personal data against accidental or

unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. Where processing is carried out by a data processor on the data controller's behalf, the data controller is also responsible for choosing a processor that provides sufficient technical and organizational measures governing the processing to be carried out.

The following sections summarize some of the key data protection principles that customers generally consider in this context, including information to help you consider AWS as your data processor in accordance with the BDSG. For ease of reference, provisions of the appendix to Section 9 BDSG are referred to in the same order that they appear in the BDSG. We also discuss aspects of the AWS services relevant to these principles. For the purposes of this discussion, we assume that the customer will be the data controller. However, as mentioned above we acknowledge that there are many circumstances where the customer could be the data processor.

Customer Control Over Content

Customers maintain control over their customer content within the AWS environment. Using AWS, customers can do the following:

- Determine where their content will be located, for example the type of storage they use on AWS and geographic location (in Europe by Country) of that storage and exclude use of other regions.
- Control the format, structure and security of their content, including whether it is masked, anonymized or encrypted. AWS offers customers options to implement strong encryption for their customer content in transit or at rest; and also provides customers with the option to manage their own encryption keys or use third party encryption mechanisms of their choice
- Manage other access controls, such as identity access management, permissions and security credentials
- Control the network setup and structure including the network security measures to prevent unauthorized access and track any access and alteration of data.

This allows AWS customers to control the entire life-cycle of their customer content on AWS, and manage their customer content in accordance with their

own specific needs, including content classification, access control, retention and deletion.

Appendix to Section 9 BDSG

1. Access Control (unauthorized access to data centres)

> Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)

AWS

AWS has implemented measures to maintain the physical security of the facilities. Currently, these measures include the following:

- Physical components of the AWS network (meaning AWS data centre facilities, servers, networking equipment, and host software systems that are used to provide the Services) are housed in nondescript facilities.
- Physical barrier controls are used to prevent unauthorized entrance to these facilities both at the perimeter (e.g., fencing, walls) and at building access points.
- Physical access points to server locations are managed by electronic access control devices and are secured with intrusion detection devices that sound alarms if the door is forced open or held open.
- Physical access is approved by an authorized individual and is revoked within 24 hours of the employee or vendor record being deactivated.
- All visitors are required to present identification and are signed in and escorted by authorized staff.
- Use of video cameras (CCTV) to monitor individual physical access to sensitive areas.
- AWS data centres utilize trained security guards 24x7, who are stationed in and around the building.

2. Access Control (unauthorized use of data processing systems)

AWS

AWS has implemented measures to maintain the security of the AWS network. Currently, these measures include the following:

- User and administrator access to the AWS network is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
- User access to the AWS network is not activated unless an active record is created in the HR System by Human Resources.
- AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
- IT access privileges are reviewed on at least a quarterly basis by appropriate personnel. In addition, access privileges are promptly revoked when the business need for access is achieved.
- Access to systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
- First time passwords/passphrases are set to a unique value and changed immediately after first use.
- User passwords/passphrases are changed at least every 90 days and only allow complex passwords (e.g. simple password variations (such as changing a single digit) are not permitted).
- Time stamped logging of any addition, deletion, and modification of user IDs, credentials, and other identifier objects is in place.
- Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.
- AWS Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
- AWS Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours.

- Communication on the AWS network is only carried out by using SSH public-key authentication through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review.

Customer

AWS offers customers various options in the Management Console to implement controls and also enables customers to implement own measures. Customer is responsible for implementing and maintaining measures on top of the AWS network, in particular with regard to configuring the architecture of the solution through the Management Console provided by AWS or other Service interfaces, as well as with regard to installing and configuring the platform and applications appropriately to customer's individual requirements. This includes without limitation measures to manage user credentials to access the Service interfaces on behalf of the customer.

In addition, customer may encrypt its data in transit and at rest. For details, see the AWS Security Best Practices whitepaper.

- **Protect your data in transit.** Cloud applications often communicate over public links, such as the Internet, so it is important to protect data in transit when you run applications in the cloud. This involves protecting network traffic between clients and servers, and network traffic between servers.

  Services from AWS provide support for both IPSec and SSL/TLS for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

- **Protect your data at rest.** Security measures that rely on encryption require keys. In the cloud, as in an on-premises system, it is essential to keep your keys secure.

  You can use existing processes to manage encryption keys in the cloud, or you can leverage server-side encryption with AWS key management and storage capabilities.

If you decide to use your own key management processes, you can use different approaches to store and protect key material. We strongly recommend that you store keys in tamper-proof storage, such as Hardware Security Modules. Amazon Web Services provides an HSM service in the cloud, known as AWS CloudHSM. Alternatively, you can use HSMs that store keys on premises, and access them over secure links, such as IPSec virtual private networks (VPNs) to Amazon VPC, or AWS Direct Connect with IPSec.

3. Access Control (unauthorized use of data)

AWS

AWS has implemented and maintains measures to control access rights for AWS employees and contractors in relation to the AWS. These measures include the following:

- User and administrator access to the AWS network is based on a role based access rights model. A unique ID is assigned to ensure appropriate user-authentication management for users and administrators on all system components.
- AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
- IT access privileges are reviewed on at least a quarterly basis by appropriate personnel.
- Time stamped logging of any addition, deletion, and modification of user IDs, credentials, and other identifier objects is in place.
- An incident response plan is in place to address the following at time of incident:
    - Roles, responsibilities, communication and contact strategies in the event of a compromise.
    - Specific incident response procedures.
    - Coverage and responses of all critical system components.

Customer

AWS offers customers various options in the Management Console to implement controls and also enables customers to implement own measures. Customers are responsible for measures addressing layers on top of the AWS network, in particular with regard to implementing and maintaining measures to control access rights to personal data.

Customers may encrypt their data in transit and at rest. For details, see the AWS Security Best Practices whitepaper (in particular the information provided in section 2. above).

The AWS Security Best Practices whitepaper also contains the following relevant information that will help you administer accounts and access rights:

- **AWS account.** This is the account that you create when you first sign up for AWS. Your AWS account represents a business relationship between you and AWS. You use your AWS account to manage your AWS resources and services. AWS accounts have root permissions to all AWS resources and services, so they are very powerful. Do not use root account credentials for day-to-day interactions with AWS. In some cases, your organization might choose to use several AWS accounts, one for each major department, for example, and then create IAM users within each of the AWS accounts for the appropriate people and resources. See also the IAM Best Practices recommendations at http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html.
- **IAM users.** With IAM you can create multiple users, each with individual security credentials, all controlled under a single AWS account. IAM users can be a person, service, or application that needs access to your AWS resources through the management console, CLI, or directly via APIs. Best practice is to create individual IAM users for each individual that needs to access services and resources in your AWS account. You can create fine-grained permissions to resources under your AWS account, apply them to groups you create, and then assign users to those groups. This best practice helps ensure users have least privilege to accomplish tasks.

  Customers are responsible for regularly reviewing accounts and access rights.

4. Disclosure Control

zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)

AWS

AWS has implemented measures in order to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons under their electronic transmission, or during their transport or recording on data carriers, and to guarantee that it is possible to examine and establish where personal data are or have had to be transmitted by data transmission equipment. Currently, these measures include the following:

- **Prevention of unauthorized copying:** The measures taken by AWS to prevent unauthorized copying of the physical storage infrastructure as such (e.g. copying customer´s data by transferring them to an external storage medium as a hard drive) are included in sections 1-3 above. In addition, personal electronic devices and removable media are prohibited from connecting to AWS information systems.
- **Use of role based access rights model:** described above.
- **Firewall policies:** described above
- **Implement an incident response plan:** described above.
- **Storage Device Decommissioning:** When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer content from being exposed to unauthorized individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices and applicable data protection law.
- **Secure Access Points:** AWS has a limited number of access points to the cloud. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows Customer to

establish a secure communication session with customer's storage or compute instances within AWS.

- **Transmission Protection:** Customer can connect to an AWS access point via HTTP or HTTPS, that is designed to protect against eavesdropping, tampering, and message forgery. For customers who require additional layers of network security, AWS offers the Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud, and the ability to use an IPsec Virtual Private Network (VPN) device to provide an encrypted tunnel between the Amazon VPC and customer's data centre.
- **Connections to AWS network by AWS personnel:** AWS personnel connect to the AWS network using SSH public-key authentication through a bastion host that restricts access to network devices and other cloud components.

Customer

AWS offers customers various options in the Management Console to implement controls, and also enables customers to implement own measures. Customers are responsible for measures addressing layers on top of the AWS network, in particular for implementing measures to ensure that the personal data transmitted by customers cannot be read, copied, modified or deleted without authorisation of customer during electronic transmission, transport or storage within the Services.

Customers may encrypt their data in transit and at rest. For details, see the AWS Security Best Practices whitepaper (in particular the information provided in section 2. above).

The AWS Security Best Practices whitepaper also provides information on Amazon Virtual Private Cloud (VPC):

- With Amazon Virtual Private Cloud (VPC) you can create private clouds within the AWS public cloud.
- Each customer Amazon VPC uses IP address space, allocated by customer. You can use private IP addresses (as recommended by RFC 1918) for your Amazon VPCs, building private clouds and associated networks in the cloud that are not directly routable to the Internet.

- Amazon VPC provides not only isolation from other customers in the private cloud, it provides layer 3 (Network Layer IP routing) isolation from the Internet as well.

5. Input Control

> zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

AWS

AWS has implemented measures in order to ensure that it is subsequently possible to verify and establish whether and by whom personal data has been entered into data processing systems, altered or removed. Currently, these measures include the following:

- **Data input not part of the Services:** The AWS services to be used by the customer under this Agreement are only infrastructure services, they do not include AWS entering any personal data on the AWS network for the customer.
- **Tracking of API Calls:** At present, AWS enables customers to trace API calls occurring under the AWS Enterprise Account. This is done by AWS providing the web service cloud trail to customer.
- **Logging and Monitoring Auditable Event Categories:** AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to continuously record the security-related events in accordance with requirements. Audit records contain a set of data elements ("When" (time stamp), "Where" (source), "Who" (user name), "What" (content)) in order to support necessary analysis requirements. In addition, audit records are available for the AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.
- **Logging User Activity:** AWS developers and administrators who need to access AWS cloud components in order to maintain them must explicitly request access. Approved AWS personnel connect to the AWS

network using SSH public-key authentication through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review.

Customer

The customer may enter personal data through the usage of the Service and is, therefore, responsible for implementing and maintaining measures for the establishment of an audit trail to document whether and by whom personal data has been entered into, modified in, or removed from processing.

Please see our AWS Risk and Compliance whitepaper for information on input control, including that, in alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type II report outlines the controls in place to manage access provisioning to AWS resources.

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. With CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

6. Instructions Control

> zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

AWS

AWS has implemented and maintains measures in order to ensure that personal data that is processed on behalf of customers can only be processed in compliance with customer's instructions. Currently, these measures include the following:

- **Internal communication:** AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees and regular management meetings for updates on business performance and other matters.
- **Amazon Corporate Segregation:** Logically, the AWS Production network is segregated from the Amazon Corporate network by means of a complex set of network security / segregation devices. AWS developers and administrators on the corporate network who need to access AWS cloud components in order to maintain them must explicitly request access. All requests are reviewed and approved by the applicable service owner. Approved AWS personnel then connect to the AWS network through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review. Access to bastion hosts require SSH public-key authentication for all user accounts on the host.
- **Robust Compliance Program:** The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, such as: SOC 1 (formerly SAS 70), SOC 2, SOC 3, and FedRAMP, PCI DSS Level 1, ISO 27001.
- **Prevention of Insider access:** AWS provides specific SOC 1 controls to address the threat of inappropriate insider access. AWS certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
- **Policies and Security Awareness Training:** AWS maintains and provides annual security awareness training to all information system users supporting AWS. Policies and procedures have been established by AWS based upon data security and data protection requirements. AWS policies, procedures and relevant training programs are reviewed by independent external auditors. Information systems administrators are bound to confidentiality and that customer content must not be processed contrary to the AWS policies, procedures and training programs.
- **Criminal Background checks:** AWS conducts criminal background checks, as permitted by applicable law, as part of employment screening

practices for employees commensurate with the employee's position and level of access to AWS facilities.

Customer

Our Services are provisioned and controlled by our customers using application programming interface (API) calls or the AWS Management Console.

Please see our Signing AWS API Requests site for more information on instructing our Services via API calls.

There are two ways you can programmatically call the functionality exposed by an Amazon Web Services (AWS) API: submit a REST/Query request over HTTP/HTTPS, or call wrapper functions in one of the AWS SDKs. This guide describes how to sign your REST/Query requests. If you use an AWS SDK, the SDK handles the signing process for you.

- **REST/Query Requests:** REST or Query requests are HTTP or HTTPS requests that use an HTTP verb (such as GET or POST) and a parameter named Action or Operation that specifies the API you are calling. Calling an API using a REST or Query request is the most direct way to access a web service, but requires that your application handle low-level details such as generating the hash to sign the request, and error handling. The benefit of using a REST or Query request is that you have access to the complete functionality of an API.
- **AWS SDKs:** The AWS SDKs provide functions that wrap an API and take care of many of the connection details, such as calculating signatures, handling request retries, and error handling. The SDKs also contain sample code, tutorials, and other resources to help you get started writing applications that call AWS. Calling the wrapper functions in an SDK can greatly simplify the process of writing an AWS application.
- **Signing REST/Query Requests:** AWS requires that you authenticate every request by signing it. To sign a request, you calculate a digital signature using a cryptographic hash function. A cryptographic hash is a one-way function that returns a unique hash value based on the input. The input to the hash function includes the text of your request and your secret access key. The hash function returns a hash value that you include in the request as your signature.

After receiving your request, AWS recalculates the signature using the same hash function and input that you used to sign the request. If the resulting signature matches the signature in the request, AWS processes the request. Otherwise, the request is rejected.

For additional security, transmission of your requests is only accepted by the API if using Secure Sockets Layer (SSL) by using HTTPS. SSL encrypts the transmission, protecting your request or the response from being viewed in transit.

7. Availability Control

zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

AWS

AWS has implemented and maintains measures in order to protect data from accidental destruction or loss. Currently, these measures include the following:

- **Fire Detection and Suppression:** Automatic fire detection and suppression equipment has been installed with AWS data centres. The fire detection system utilizes smoke detection sensors in all data centre environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.
- **Redundant Power Systems:** The data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centres use generators to provide back-up power for the entire facility.
- **Climate and Temperature Control:** Personnel and systems monitor and control temperature and humidity at appropriate levels.
- **Preventative maintenance:** Preventative maintenance is performed to maintain the continued operability of equipment.
- **Multiple availability zones:** AWS provides customers with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each

availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). Availability zones are all redundantly connected to multiple tier-1 transit providers.

- **Executive Review of contingency plans:** The AWS contingency plans are periodically reviewed by members of the Senior Executive management team and the Audit Committee of the Board of Directors.

Customer

AWS offers customers various options in the Management Console to implement controls and also enables customers to implement their own measures. Our customers are responsible for properly designing and configuring the architecture using the Service Offerings in order to meet customer's requirements with regard to the availability of personal data (e.g. by adding redundancy and configuring suitable archiving / backup concepts depending on the criticality of its data / configuring logical architecture as a 3 tier based approach). We recommend that customers create regular backups of customer content and maintain industry standard measures against unauthorized access, deletion or accidental loss of customer content. Additionally, customer should have policies in place which enforce the usage of antivirus and firewall software on systems used to access the Service Offerings or customer content.

8. Separation Control

zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

(Trennungskontrolle)

AWS

AWS has taken the following technical and organizational measures in order to ensure that data collected for different purposes are processed separately:

- **Multi-tenant environment:** The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, security controls designed to isolate each customer from other

customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines.

- **Single-tenancy option:** AWS services, e.g. Virtual Private Cloud (VPC), allow customers to use instances that are physically isolated at the host hardware level or isolate the AWS services from the Internet; they will run on single tenant hardware.
- **Amazon Corporate Segregation:** described above.
- **Unique encryption key:** AWS customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant.

Customer

Our customers retain control and ownership of their data and may implement a labelling and handing policy and procedures to meet their requirements. For more information, see the AWS Risk and Compliance whitepaper.

Segregation of Content (data) is the responsibility of our customers as customers retain ownership and control of their own guest operating systems, software, applications and data. Through configuration tools such as the AWS Management Console and APIs, customers may use service features to reinforce data separation, such as block based encryption. Customers may also use encryption tools available from third party vendors. It is the customer's responsibility to make use of such additional measures as it deems adequate to ensure the level of separation the customer requires.

Correction, Deletion, and Blocking of Content

The AWS services are provided in a way (as described in the user and admin guides for the Services located at http://aws.amazon.com/documentation) that gives customers the option to implement controls to retrieve, correct, delete, or block customer content.

When a customer deletes its content from the AWS services, the content is rendered unreadable or disabled and the underlying storage areas on the AWS network that were used to store the content are wiped prior to being reclaimed and overwritten in accordance with AWS standard policies and deletion timelines.

AWS does not correct, delete or block customer content without the agreement of the customer.

Subcontractors

AWS uses a number of third party subcontractors to assist with the provision of its services. Our subcontractors do not have logical access to customer content. In addition, AWS only uses subcontractors that we trust and we use appropriate contractual safeguards which we monitor to ensure the required standards are maintained. Details of any subcontractors who have access to customer content, including personal data, are set out on the AWS website.

Data Breaches

Given that customers maintain management of and control over personal data when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.

Customers control their own access keys and determine who is authorized to access their AWS account. AWS does not have visibility of access keys, or who is and who is not authorized to log into an account; therefore, the customer is responsible for monitoring use, misuse, distribution or loss of access keys.

AWS will promptly notify the customer if AWS has actual knowledge of a confirmed breach of the AWS security standards relating to the AWS network.

Deletion on Termination

The AWS services empower the customer to make choices about deletion. As the AWS services are self-service, they merely respond automatically to the

customer's instructions, which the customer inputs via the AWS Management Console or the APIs.

If the customer wants to delete customer content (whether in the course of using the AWS services or when it stops using the AWS services), the customer must use the AWS Management Console or the APIs to instruct the AWS services to delete each instance of customer content which the customer wants to delete.

AWS does not manage or choose to delete customer content on the customer's behalf.

The customer is empowered to choose the format the customer content is in when the customer puts that content through the AWS deletion process. This gives the customer complete control to enhance the protection around the customer content that it wants to delete.

To further protect customer content that it chooses to delete:

- Where applicable to the service, the customer could wipe customer content before deleting it.
- The customer could encrypt customer content before deleting it.

If the customer deletes customer content in an encrypted format, then it will remain encrypted throughout the AWS deletion process. Without the encryption key it will be impossible to decrypt this data. To enhance protection, customer can also choose to store the encryption key outside the AWS environment and destroy it to prevent decryption.

Even if the encryption key were available, decryption would be extremely unlikely because:

- The customer content is stored across different storage media in the relevant AWS Region and the mapping between the different storage media is eliminated when the customer chooses to delete the data.
- At any time after the customer deletes the customer content individual parts of that data may be overwritten because the storage media hosting it is re-provisioned and, depending on how the data is structured, it may not be possible to decrypt without all the data.

Customer's Third Party Service Providers

As referred to earlier in this document, the AWS environment is also connected to other services provided directly by third parties to the customer (for example, Internet Service Providers). These third parties retain responsibility over their own systems, including for security, and AWS is not responsible for the activities of these third parties.

Other Considerations

This Whitepaper does not discuss other privacy related laws, aside from the BDSG, that may also be relevant to customers, including any industry specific requirements such as special requirements for banks, insurance companies, doctors and hospitals etc. The relevant privacy and data protection laws and regulations applicable to individual customers will depend on several factors including where a customer conducts business, the industry in which it operates, the type of content they wish to store, where or from whom the content originates, and where the content will be stored.

Customers concerned about their privacy regulatory obligations should first ensure they identify and understand the requirements applying to them, and seek appropriate advice.

Conclusion

For AWS, security is our top priority. We deliver services to more than one million active customers, including enterprises, educational institutions and government agencies in over 190 countries. Our customers include financial services providers and healthcare providers, and we are trusted with some of their most sensitive information, including personal health data and financial records.

AWS services are designed to give customers flexibility over how they configure and deploy their solutions as well as control over their content, including where it is stored, how it is stored and who has access to it. AWS customers can build their own secure applications and store content securely on AWS.

Further Reading

To help customers further understand how they can address their privacy and data protection requirements, customers are encouraged to read the risk, compliance and security whitepapers, best practices, checklists and guidance published on the AWS website. This material can be found at http://aws.amazon.com/compliance and http://aws.amazon.com/security.

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS cloud and gain proficiency with AWS services and solutions. We offer free instructional videos, self-paced labs, and instructor-led classes. Further information on AWS training is available at http://aws.amazon.com/training/.

AWS certifications certify the technical skills and knowledge associated with best practices for building secure and reliable cloud-based applications using AWS technology. Further information on AWS certifications is available at http://aws.amazon.com/certification/.

If you require further information, please contact AWS at: https://aws.amazon.com/contact-us/ or contact your local AWS account representative.

Document Revisions

Date	Description
January 2017	First publication