Whitepaper on EU Data Protection

December 2016

Please see http://aws.amazon.com/compliance/aws-whitepapers/ for the latest version

Introduction

This document provides information to assist customers who want to use AWS to store content containing personal data. Specifically, this document describes how customers can use AWS services in compliance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive"). It aims to help customers understand:

- The way AWS services operate, including how customers can comply with EU law, address their security needs and encrypt and otherwise protect their content
- The customer's complete control over the geographic locations where their content can be stored and accessed, and other relevant compliance considerations
- The respective roles the customer and AWS each play in managing and securing content stored on AWS services

This whitepaper focuses on typical questions asked by AWS customers when considering the implications of the Directive on their use of AWS services to store content including personal data. There will also be other relevant considerations for each customer to address, such as the customer's need to comply with industry specific requirements and the laws of other jurisdictions where that customer conducts business. This paper is provided for the purposes of 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 environments, and more generally, applicable laws relevant to their business.

Considerations Relating to Customer Content

Storage of content presents all organisations with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?
- Who will have access to content?
- What laws and regulations apply to the content and what is needed to comply with these?

These considerations are not new and they are not cloud-specific. They are relevant to internally hosted and operated systems as well as traditional third party hosted services. When using AWS services, customers maintain control over their content and are responsible for – and fully enabled to -- manage and control their individual content security requirements, including:

- What content they choose to store on AWS
- Whether that content will be encrypted – at rest and in transit
- Which AWS services are used with the content
- Where in the world that content is stored and processed
- The format and structure of that content and whether it is masked or anonymised
- Who they allow to access that content and how those access rights are granted, managed and revoked

Security of the customer's content relies on both AWS and the customer to implement appropriate measures. While AWS implements security controls in its underlying cloud environment, AWS customers retain control over their content and the security of that content. Understanding the respective and differing roles of the customer and AWS is fundamental in the context of the data protection requirements that may apply to personal data stored on AWS.

Security of Customer Content:

Moving IT infrastructure to AWS means that 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 management of 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 the 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 centers.

This model is shown below in Figure 1:

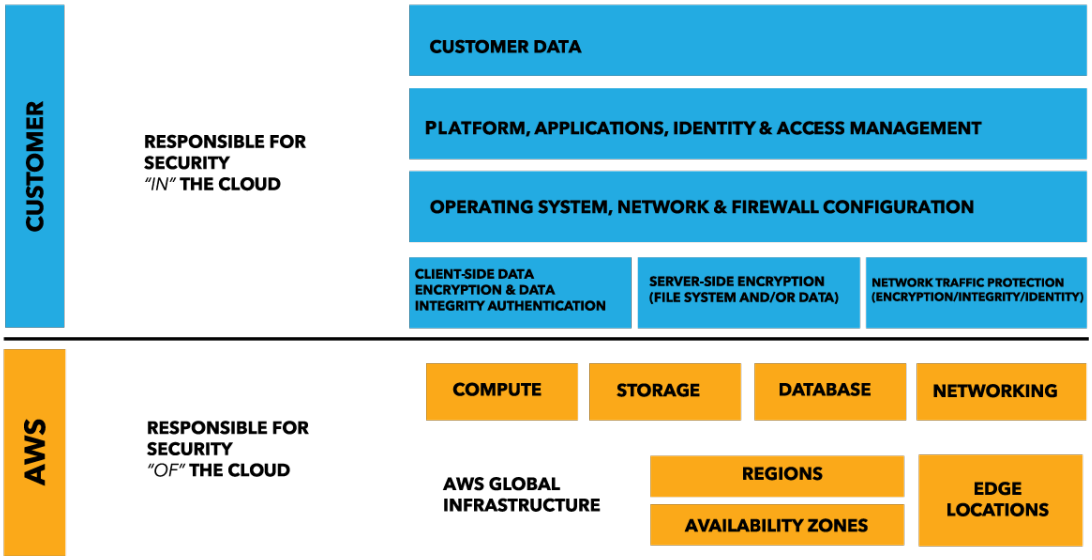

Figure 1 – Security Model

What does this model mean for the security of 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"; 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 content, platform, applications, systems and networks – 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. This is a key difference to traditional hosting solutions where the provider 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 higher 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.

Understanding security OF the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS cloud infrastructure has been constructed to be one of the most flexible and secure cloud computing environments available, designed to provide optimum availability while offering complete customer segregation. It provides an extremely scalable, highly reliable platform that enables customers to deploy applications and content quickly and securely at massive global scale if necessary. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which they store their content. Because AWS does not know what data customers are storing in AWS services, AWS cannot distinguish personal data from any other type of data stored by a customer as part of that customer's content.

AWS' world-class, highly secure data centres utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centres are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis, limited to system administration purposes. For a comprehensive list of all the security measures built into the core AWS cloud infrastructure, platforms, and services, please read our Overview of Security Processes whitepaper.

We are vigilant about the security of our underlying cloud environment, and have implemented sophisticated technical and organisational measures against unauthorized access. 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 and 2 reports, ISO 27001 certification 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 applicable AWS compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found at the AWS compliance site.

AWS provides a data processing addendum to help customers meet their data protection obligations. AWS can also add the Standard Contractual Clauses 2010/87/EU (often referred to as "Model Clauses") to a customer's data processing addendum if the customer needs this to transfer personal data from the EU to a country outside the European Economic Area.

On March 6, 215, 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. This approval means that any AWS customer who requires the Model Clauses can now rely on the AWS data processing addendum as providing sufficient contractual commitments to enable international data flows in accordance with the Directive. For more detail 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

In addition to the data processing addendum and the Model Clauses, customers who wish to transfer their personal data from AWS' EU regions to US regions benefit from AWS' participation in the EU-U.S. Privacy Shield Framework. Amazon.com, Inc., along with certain of its U.S. affiliates, including AWS, was certified under the EU-U.S. Privacy Shield Framework on October 21, 2016. The EU-U.S. Privacy Shield Framework does not affect the way customers use, or work with, AWS, but, rather, provides an additional, EU-sanctioned mechanism for transferring personal data from the EU to the US. For details on the obligations for US service providers under the EU-U.S. Privacy Shield Framework, please see the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm and the EU-U.S. Privacy Shield Framework website here: https://www.privacyshield.gov/welcome.

Understanding security IN the cloud

Customers retain control of their content when issuing AWS services. Customers, rather than AWS, determine what content they store in AWS, control how they configure their environments and secure their content, whether they will encrypt their content at rest and in transit, who will access that content and what credentials will be required (including use of multi-factor authentication), and what additional security features and tools they use and how they use them.

Because our customers retain control over their security, they also retain responsibility for the security of anything their organisation puts on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platform and database services.

Customers can configure their AWS services to leverage a range of optional security features, tools and controls to protect their content, including sophisticated identity and access management tools, availability configurations, backup capabilities, security capabilities, encryption and network security. To assist customers in designing, implementing and operating their own secure AWS environment, AWS provides a wide array of security features customers can use. Customers can also use their own or third party security tools and controls. Examples of steps customers can take to help secure their content include implementing:

- Strong password policies, assigning appropriate permissions to users and taking robust steps to protect their access keys
- Appropriate firewalls and network segmentation including Virtual Private Cloud, encrypting content, use of SSL and properly architecting systems to decrease the risk of data loss and unauthorized access
- Appropriate redundancy schemes and backup strategies to mitigate the risk of data loss or unavailability

All of these factors are within customers' control, rather than AWS's. AWS does not have any visibility into the content customers are placing on AWS and does not change customer configuration settings; they are determined and controlled by the customer. Since it is the customers who decide what content to place in the AWS cloud, only the customer can determine what level of security is appropriate for the data which is stored there.

To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and execute security assessments of their organisation's use of AWS services, AWS publishes a number of whitepapers relating to security, governance, risk and compliance; and a number of checklists and best practices. Customers are also free to design and execute security assessments according to their own preferences, and can request permission to conduct scans of their cloud infrastructure (provided those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy).

AWS Regions

AWS data centres are built in clusters in various countries around the world. We refer to each of our data center 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), the UK (London) and Germany (Frankfurt). Customers can choose to use one Region, all Regions or any combination of Regions. Figure 2 shows AWS Region locations:

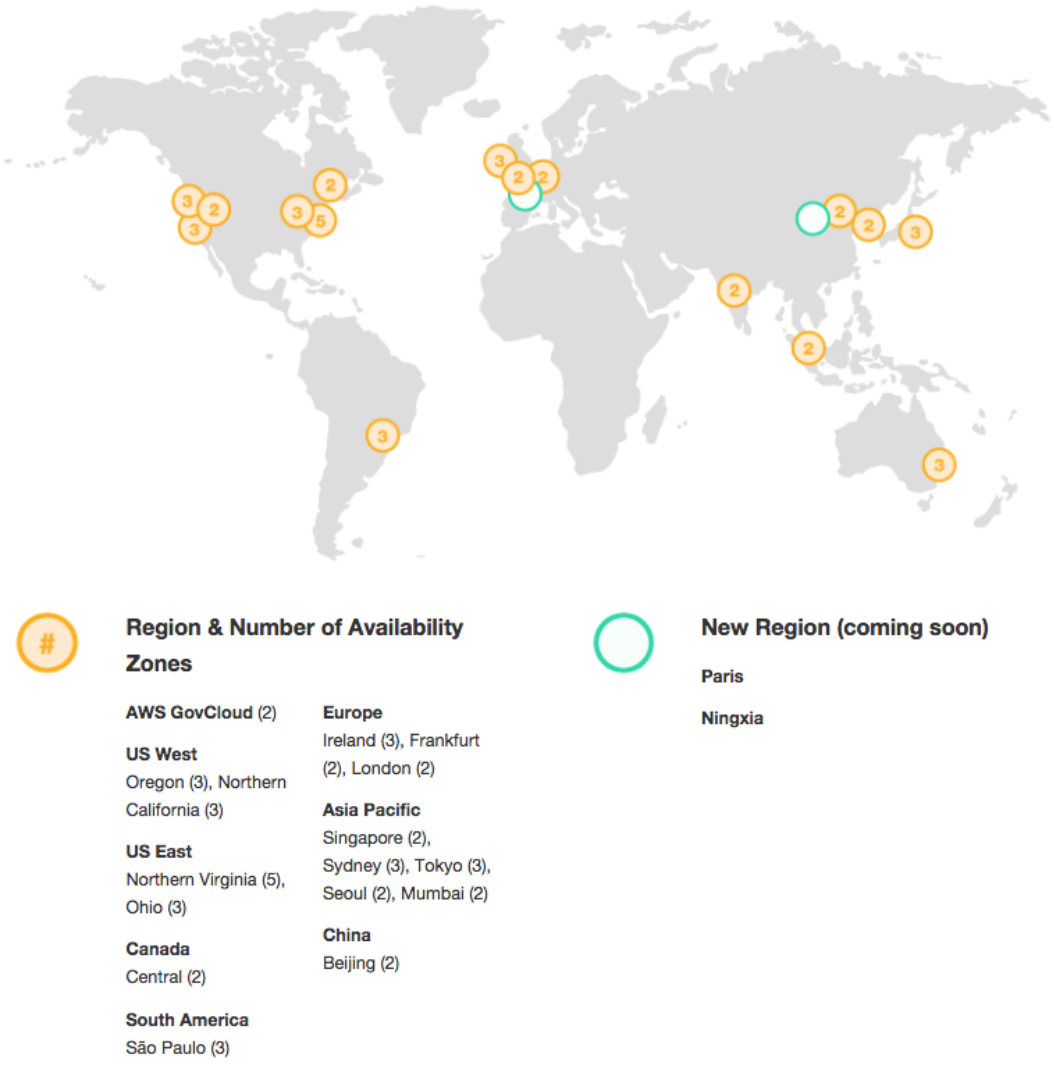

Figure 2 – AWS Global Regions

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 (Germany) Region. If the customer makes this choice, their content will be stored in Germany unless the customer selects a different AWS Region.

Customers can replicate and back up content in more than one Region, but AWS does not move customer content outside of the customer's chosen Region(s).

How can customers select their Region(s)?

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 3: 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.

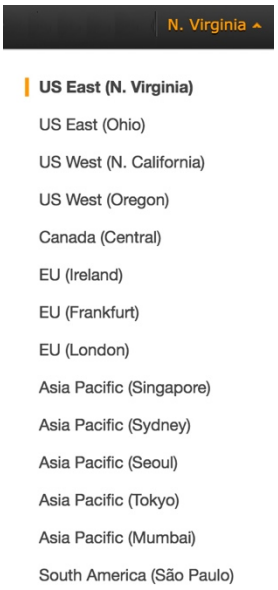

Figure 3 – Selecting AWS Global Regions in the AWS Management Console

Customers can also prescribe the AWS Region to be used for their compute resources by taking advantage of the Amazon Virtual Private Cloud (VPC) capability. Amazon VPC lets the customer provision a section of the AWS cloud where the customer can launch AWS resources in a virtual network that the customer defines. With 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.

Customer Controls and Access to Customer Content

Customer control over content

Customers using AWS maintain control over their content within the AWS environment. They can:

- Determine where it will be located, for example the type of storage environment and geographic location of that storage
- Control the format of that content, for example plain text, masked, anonymised or encrypted, using either AWS provided encryption or a third-party encryption mechanism of the customer's choice

- Manage other access controls, such as identity access management and security credentials
- Control whether to use SSL, Virtual Private Cloud and other network security measures to prevent unauthorised access

This allows AWS customers to control the entire life-cycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion.

Access to customer content

AWS does not access any customer's content except as necessary to provide that customer with the AWS services it has selected. AWS does not access customers' content for any other purposes.

AWS does not know what content customers choose to store on AWS and cannot distinguish between personal data and other content, so AWS treats all customer content the same. In this way, all customer content benefits from the same robust AWS security measures, whether this content includes personal data or not. AWS simply makes available 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. Customer is then free to build on that infrastructure security based on the customer's own, unique requirements.

Government rights of access

Queries are often raised 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). However, it is important to remember that 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 authorised. 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.

Most countries have data access laws which purport to have extraterritorial application. An example of a US law with extra-territorial reach that is often mentioned in the context of cloud services is the U.S. Patriot Act. The Patriot Act is not dissimilar to laws in many other developed nations that enable governments to obtain information with respect to investigations relating to international terrorism and other foreign intelligence issues. Any request for documents under the Patriot Act requires a court order demonstrating that the request complies with the law, including, for example, that the request is related to legitimate investigations.

AWS Policy

Regardless of where a request for customer content comes from or who the customer is, AWS is always vigilant about protecting our customers' content. 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 typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. We carefully examine each request to authenticate its accuracy and verify that it complies with applicable law. We will challenge requests that are overbroad, exceed the requestor's authority or do not fully comply with applicable law. If we are compelled to disclose customer content, we notify customers before disclosure to provide them with the opportunity to seek protection from disclosure, unless prohibited by law.

Data Protection in the EU: The Directive

We consider below the obligations contained in the Directive[1]. Broadly, the Directive sets out a number of data protection requirements which apply when personal data is being processed. In this context "processing" includes any operation or set of operations which is performed upon personal data. Under the Directive, "personal data" is defined as information from which a living individual may be identified or identifiable (known as the "data subject"). In addition, the Directive makes a distinction between (a) the "data controller" – the party which determines the purposes and means of the processing of personal data, and (b) a "data processor" – a party which processes personal data on behalf of the controller.

It is the data controller that must ensure that its processing of personal data complies with the data protection obligations. For example, the data controller needs to ensure that the personal data is being processed fairly and lawfully, and that the data is secured against unauthorised or unlawful processing.

[1] We should keep in mind that the Directive does not apply to organisations established in the EU Member States directly. Instead, the EU Member States are required to implement the Directive in their national legislation. As a consequence, there may be some variations between the precise nature of the obligations in different Member States, so customers should seek advice as to which national laws apply to them.

AWS appreciates that its services are used as part of a variety of different business operations, and there may be multiple parties involved in a chain of supply. As a general guide, however, where personal data is included in customer content that is stored 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 data will be processed and has chosen how it will be processed.
- 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)

As a provider of self-service infrastructure that is completely under the customers' control – including with respect to how and whether the data is "processed", AWS only provides the infrastructure services for customers who want to upload and process content on the AWS network. In this context, AWS does not have any visibility into or knowledge of what customers are uploading onto its network, including whether or not that content includes any personal data. AWS customers are also empowered to use encryption to render content unintelligible for AWS. AWS does not process customer content except as necessary to provide the services (or to comply with the law or a valid and binding order).

AWS also has systems, procedures and policies in place to prevent any access to customer content by AWS employees. Additionally, for customers who wish to process personal data, AWS provides a data processing addendum to help customers meet their data protection obligations. AWS can also add the Model Clauses to a customer's data processing addendum if the customer needs this to transfer personal data from the EU to a country outside the European Economic Area.

On March 6, 215, 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. This approval means that any AWS customer who requires the Model Clauses can now rely on the AWS data processing addendum as providing sufficient contractual commitments to enable international data flows in accordance with the Directive. For more detail 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

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.

We summarise in the table below some of the key data protection principles that customers generally consider in this context. We also discuss aspects of the AWS services relevant to these principles. For the purposes of this table, we have assumed that the AWS customer will be the data controller. However, as mentioned above we acknowledge that there are many

circumstances where the AWS customer will be the data processor. In these situations, however, the AWS customer may still find the below useful in the context of its own relationship with the controller.

Data Protection Principle	Summary of Data Protection Obligation	Considerations
Fairness	Data subjects should be given accurate and full information about the identity of the controller, the purposes of the processing, and any other Information necessary to guarantee fair processing.	**Customer:** It is the customer (or their customer) who decides what information it collects and for what purposes this information is used. In many cases, the customer will have a direct relationship with any data subjects, and so will be best placed to communicate directly with them. Further, the customer should know the scope of any notice which has previously been given to the data subjects. **AWS:** AWS has no control over what types of content the customer chooses to store in AWS and for what purpose. AWS also has no insight into this content (including whether or not it includes personal data). AWS has no means of identifying data subjects or contacting data subjects whose personal data the customer has chosen to store in on the AWS infrastructure, and is therefore not able provide any information to the relevant data subjects.
Lawful basis	The controller must have a lawful basis for its processing, which satisfies at least one of the criteria set out in the Directive.	**Customer:** When deciding whether and for what purpose it will process personal data, the customer will need to consider whether it satisfies one of the criteria in the Directive. These include, for example, that the data subject has given his consent, or that the processing is necessary for the performance of a contract to which the data subject is a party. **AWS:** As stated above, AWS has no control over what types of content the customer chooses to store in AWS (including whether or not it includes personal data). AWS does not determine what architecture the customer elects to build by combining the AWS service offerings and whether or not it is appropriate for the customer's specific needs. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed. Accordingly, AWS is not able to ascertain whether there may be a lawful basis for the processing.

Purpose Limitation	Personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.	**Customer:** It is the customer who determines what personal data it collects and what purposes it will be used for. When making this decision, the customer must ensure that it has a specified, explicit and legitimate purpose. The customer decides whether the data will be subsequently processed for any other purposes, and can make an assessment as to whether these are compatible with the initial purpose. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. To the extent that the customer content contains personal data, AWS only processes that data to provide the AWS services selected by each customer to that customer (except in the limited cases where required to comply with law or a valid and binding order).
Rights of data subjects	Data subjects must be able to access their personal data, and obtain the rectification, erasure or blocking of personal data which is processed otherwise than in accordance with the Directive.	**Customers:** The customer retains control of content stored on AWS, and therefore can decide how data subjects may access any of their personal data included in that content. Similarly, it is the customer who is best placed to be able to respond to a request or complaint from a data subject regarding the lawfulness of the customer's data processing activities. **AWS**: As explained above, AWS has no control over what types of content the customer chooses to store in AWS and for what purposes. AWS has no insight into this content (including whether or not it includes personal data). AWS cannot identify and has no contact with data subjects whose personal data the customer has chosen to store in AWS (except in cases where this relates to the customer him/herself), and is therefore not able provide any information to the relevant data subjects. AWS has no ability to connect data stored on AWS with any particular person. That information is exclusively in the customers' control.
Accuracy	Data controllers must ensure that personal data is accurate and, where necessary, kept up to date.	**Customers:** The customer has control over the personal data which it chooses to store on AWS. It is therefore responsible for verifying and maintaining its accuracy (and can update and correct it as necessary). In addition, the customer manages and is responsible for the security 'in' the cloud, and so the customer is able to ensure that it has implemented appropriate measures to protect against corruption of the data.

		AWS: AWS has no control over what types of content the customer chooses to store in AWS, and no insight into this content. AWS does not enter or modify any data on the customer's behalf. It is therefore unable to verify the accuracy of this data or update it. However, SOC 1 Type 2 report includes details of the controls that AWS maintains to ensure the integrity of the data at the level of the underlying cloud environment.
Data Security	Data controllers must implement appropriate technical and organisational measures to protect personal data from accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.	**Customers:** Only the customer is in a position to determine whether any particular security architecture it designs or implements is appropriate to any particular type of content including any personal data. Customers are responsible for security ***in*** the cloud, including security of their content (and any personal data included in their content) and implementing an appropriate architecture using the AWS service offerings. In particular, customers are responsible for properly (a) configuring the AWS services, (b) using the controls available in connection with the services, and (c) taking such steps as they consider necessary to maintain appropriate security controls and backup of their personal data (e.g. by using encryption technology to protect the personal data from unauthorized access, and routine archiving). **AWS:** AWS is responsible for managing the security ***of*** the underlying cloud environment. For a complete list of all the security measures built into the core AWS cloud infrastructure, platforms, and services, please read our Overview of Security Processes[3] whitepaper. AWS uses external auditors to verify the efficacy of its security measures, including the security of the physical data centres from which AWS provides its services. Upon customers' written request and signature of an NDA, AWS will provide customers with a summary of the auditors' report so that customers can reasonably verify AWS security measures. AWS will also provide this summary to Data Protection Authorities on request.

Data Retention	Personal data should not be kept (in an identifiable form) for longer than is necessary for the purposes for which the personal data was collected or further processed.	**Customers:** It is the customer who decides what purposes any personal data stored in the AWS cloud will be used for, and accordingly for how long it is necessary to retain that personal data. The customer can delete or anonymize the personal data when it is no longer needed. **AWS:** AWS has no insight into whether stored data includes personal data or to the purposes for which the customer is processing any particular data which it has stored in the cloud. Accordingly, it cannot determine for how long it is necessary to retain the data in order to achieve that purpose. 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 procedures also include a secure decommissioning process conducted prior to disposal of storage media used to provide the AWS services. As part of that process, storage media is degaussed or erased and physically destroyed or disabled in accordance with industry standard practices.
Transfer	Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	**Customer:** The customer can choose the AWS Region(s) in which their content and servers will be located. The customer can choose to deploy their AWS services exclusively in the AWS EU Regions in Germany, the UK or Ireland. **AWS:** AWS does not move customer content outside of the customer's chosen Region(s) except as necessary to comply with the law or a valid and binding order, AWS provides a data processing addendum to help customers meet their data protection obligations. AWS can also add the Model Clauses to a customer's data processing addendum if the customer needs this to transfer personal data from the EU to a country outside the European Economic Area. On March 6, 215, 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. This approval means that any AWS customer who requires the Model Clauses can now rely on the AWS data processing addendum as providing sufficient contractual commitments to enable international data flows in accordance with the Directive.

		For more detail 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 In addition to the data processing addendum and the Model Clauses, customers who wish to transfer their personal data from AWS' EU regions to US regions benefit from AWS' participation in the EU-U.S. Privacy Shield Framework. The EU-U.S. Privacy Shield Framework does not affect the way customers use, or work with, AWS, but, rather, provides an additional, EU-sanctioned mechanism for transferring personal data from the EU to the US. For details on the obligations for US service providers under the EU-U.S. Privacy Shield Framework, please see the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm and the EU-U.S. Privacy Shield Framework website here: https://www.privacyshield.gov/welcome.

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.

Where required by applicable law, 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.

Subcontractors

AWS uses a number of third-party subcontractors to assist with the provision of it service. However, our subcontractors do not have access to customers' 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.

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 (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 Directive, that may also be relevant to customers, including any industry specific requirements. 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.

Final Comments

For AWS, security is always our top priority. We deliver services to hundreds of thousands of businesses 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.

Additional Resources

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.