Supporting customers in the context of DiGAV compliance

FAQs

Published 6 October 2021

Notices

Are AWS services GDPR compliant?
All AWS services can be used in compliance with GDPR. This means that, in addition to benefiting from all of the measures that AWS already takes to maintain security of the AWS services, customers can deploy AWS services as a key part of their GDPR compliance plans. For more details, see our GDPR Center.

Does the German DiGAV require personal data to only be processed within the EEA?
Customers seeking to be eligible for reimbursement under the German Digital Supply Act (DVG) and Digital Health Applications Ordinance (DiGAV) must demonstrate that personal data is processed within the EEA or countries with an adequacy decision from the EU Commission.

Can AWS services be used in compliance with DiGAV?
Yes. Depending on the architecture and AWS services chosen by the customer, it is possible to use AWS services in compliance with DiGAV requirements. AWS does not determine the location of customer data and only processes data based on the documented instructions of its customers. Customers retain complete control and ownership of their data when they choose the region in which their data is physically located. AWS customers interested in developing or operating applications under DiGAV may select AWS regions and services to meet the requirements of DiGAV, including in the AWS Europe (Frankfurt) region in Germany.

Which AWS services can I use to only process data within the EEA?
Customers can find information about the Privacy Features of AWS Services to determine which AWS services can be used without transferring data from the AWS region(s) selected by the customer. By selecting AWS services that do not transfer customer data and properly configuring those services for use from AWS regions located within the EEA, customers can enable EEA-only data processing. To help ensure appropriate configuration, technical measures (SCPs and others) can be put in place that block the usage of AWS resources in regions outside of the EEA. Please refer to the DiGAV Blueprint.

How can I use AWS services in a way that personal data is not processed outside of the EEA?
Customers select the AWS region in which their customer data will be stored. AWS will not process this customer data outside the customer's selected AWS region except as necessary to maintain or provide the AWS services, or as necessary to comply with the law or a binding order of a governmental body. Further, we prohibit, and our systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by customer, is required to prevent fraud and abuse, or to comply with law.

A small number of AWS services involve the transfer of customer data—for example, to develop and improve those services (but allowing customers to opt out of data transfers) or because transfer is an essential part of the service (such as a content delivery service). Please refer to the Privacy Features of AWS Services to determine which AWS services can be used without transferring data from the AWS region(s) selected by the customer. By selecting AWS services that do not transfer customer data and properly configuring those services for use from AWS regions located within the EEA, customers can enable EEA-only data processing.

Which documentation can I use to demonstrate EEA only data processing when using AWS services to regulatory bodies or customers?
It's the customer's responsibility to configure AWS services correctly to avoid data processing in a region outside of the EEA. AWS provides tools to ensure this as outlined in the DiGAV Blueprint which refers to the service documentation for these measures.

What infrastructure does AWS provide within the EEA?
Please see here for an overview over the AWS global infrastructure and regions, edge locations and other infrastructure within the EEA.

Can AWS support be used when EEA-only processing is intended?
Yes. We prohibit, and our systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by customer, is required to prevent fraud and abuse, or to comply with law.

The German Federal Institute for Drugs and Medical Devices (BfArM) requires commitments from international cloud providers, such as AWS, regarding the handling of foreign law enforcement requests (e.g. under the CLOUD act). Does AWS provide such commitments?
Yes. Protecting customer data is our top priority. AWS has recently strengthened our commitment to protect customer data from law enforcement requests by governmental bodies inside and outside of the EEA via a Supplementary Addendum to our GDPR DPA.

We know that transparency matters to our customers, so we regularly publish a report about the types and volume of information requests we receive, and how AWS responds to them, on the Amazon Information Requests webpage. Please see here for more information on the CLOUD act and implications for AWS customers.

Which sub-processors does AWS use to process data?
Please see a list of AWS sub-processors here.

BfArM guidance suggests encryption with customer managed encryption keys (CMEK or CMK) when using cloud providers. How can this be implemented on AWS?
AWS provides a number of advanced encryption and key management services that customers can use to protect their content. Customers can also choose from a number of supported third-party encryption solutions when using AWS services. Encrypted content is useless without the applicable decryption keys. Please see the Privacy Features of AWS Services for a list of AWS services that support encryption.

Key management services, such as AWS KMS and CloudHSM, enable customers to effectively and securely manage their encryption keys. Please get in touch with your AWS account team (or contact us here) for guidance on a CMEK based encryption solution on AWS.