General Data Protection Regulation Overview

The General Data Protection Regulation (GDPR) is a European privacy law (Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016) that became enforceable on May 25, 2018. The GDPR replaces the EU Data Protection Directive (**Directive 95/46/EC)**, and is intended to harmonize data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each EU member state.

The GDPR applies to all processing of *personal data* either by organizations that have an establishment in the EU, or to organizations that process personal data of EU residents when offering goods or services to individuals in the EU or monitoring the behavior of EU residents in the EU. Personal data is any information relating to an identified or identifiable natural person.

Changes the GDPR Introduces to Organizations Operating in the EU

One of the key aspects of the GDPR is that it creates consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organizations must demonstrate the security of the data they are processing and their compliance with the GDPR on a continual basis, by implementing and regularly reviewing technical and organizational measures, as well as compliance policies applicable to the processing of personal data. EU supervisory authorities can issue fines of up to EUR 20 million, or 4% of annual worldwide turnover, whichever is higher, for a breach of the GDPR.

AWS Preparation for the GDPR

AWS compliance, data protection, and security experts work with customers around the world to answer their questions and help them prepare to run workloads in the cloud under the GDPR. These teams also review the readiness of AWS against the requirements of the GDPR.

> **Note**
>
> We can confirm that all AWS services can be used in compliance with the GDPR.

AWS Data Processing Addendum (DPA)

AWS offers a GDPR-compliant AWS Global Data Processing Addendum (GDPR DPA), which enables customers to comply with GDPR contractual obligations. The AWS GDPR DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR whenever customers use AWS services to process personal data, regardless of which data protection laws apply to that processing.

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling regarding the EU-US Privacy Shield and Standard Contractual Clauses (SCCs), also known as "model clauses." The CJEU ruled that the EU-US Privacy Shield is no longer valid for the transfer of personal data from the European Union (EU) to the United States (US). However, in the same ruling, the CJEU validated that companies can continue to use SCCs as a mechanism for transferring data outside of the EU.

Following this ruling, AWS customers and partners can continue to use AWS to transfer their content from Europe to the US and other countries, in compliance with EU data protection laws – including the General Data Protection Regulation (GDPR). AWS customers can rely on the SCCs included in the AWS Data Processing Addendum (DPA) if they choose to transfer their data outside the European Union in compliance with GDPR. As the regulatory and legislative landscape evolves, we will work to ensure that our customers and partners can continue to enjoy the benefits of AWS everywhere they operate. An example of such an evolving scenario is the new adequacy decision on the new "EU-US Data Privacy Framework", adopted by the European Commission, on 10 July 2023. For additional information, see the EU-US Privacy Shield FAQ.

Furthermore, AWS announced strengthened contractual commitments that go beyond what's required by the Schrems II ruling and currently provided by other cloud providers to protect the personal data that customers entrust AWS to process (customer data). Significantly, these new commitments apply to all customer data subject to GDPR processed by AWS, whether it is transferred outside the European Economic Area (EEA) or not. These commitments are automatically available to all customers using AWS to process their customer data, with no additional action required, through a new supplementary addendum to the AWS GDPR Data Processing Addendum, which is also incorporated in the AWS Service Terms.

AWS has published an additional whitepaper, Navigating Compliance with EU Data Transfer Requirements, to help customers conducting both their data transfer assessments and understanding the key supplementary measures made available to protect customer data according to the recommendations released by the European Data Protection Board (EDPB).

The Role of AWS Under the GDPR

Under the GDPR, AWS acts as both a data processor and a data controller.

Under Article 32, controllers and processors are required to "…implement appropriate technical and organizational measures" that consider "the state of the art and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". The GDPR provides specific suggestions for what types of security actions may be required, including:

- The pseudonymization and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner, in the event of a physical or technical incident.
- A process to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure the security of the processing.

AWS as a Data Processor

When customers and AWS Partner Network (APN) Partners use AWS Services to process personal data in their content, AWS acts as a data processor. Customers and APN Partners can use the controls available in AWS services, including security configuration controls, to process personal data. Under these circumstances, the customer or APN Partners may act as a data controller or a data processor, and AWS acts as a data processor or sub-processor. The GDPR-compliant AWS DPA incorporates the commitments of AWS as a data processor.

AWS as a Data Controller

When AWS collects personal data and determines the purposes and means of processing that personal data, it acts as a data controller. For example, when AWS processes account information for account registration, administration, services access, or contact information for the AWS account to provide assistance through customer support activities, it acts as a data controller.