Navigating Compliance with EU Data Transfer Requirements

January 3, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. 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 provides information about services and resources that Amazon Web Services (AWS) offers customers to help them conduct data transfer assessments in light of the "Schrems II" ruling about transfers of personal data subject to the General Data Protection Regulation, and subsequent recommendations from the European Data Protection Board. This document also describes the key supplementary measures taken by AWS and made available by AWS to protect customer data.

Introduction

AWS is committed to enabling customers to use all AWS services in compliance with the EU's data protection regulations, including the General Data Protection Regulation (GDPR). This paper describes how AWS customers can continue to use AWS services in compliance with the quickly evolving data protection landscape in the EU following the Schrems II ruling and the subsequent recommendations released by the European Data Protection Board (EDPB). The steps laid out in this document outline how customers can conduct assessments of their use of the AWS services in accordance with the Schrems II ruling and the EDPB's recommendations, and as a result, enable them to comply with EU data protection regulations.

Overview of Schrems II Ruling

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling (the "Schrems II" ruling) regarding the transfer of personal data subject to GDPR outside the European Economic Area (EEA). In Schrems II, the CJEU ruled that the EU-US Privacy Shield was no longer a valid mechanism to transfer personal data from the EEA to the United States. However, in the same ruling, the CJEU confirmed that organizations can (subject to meeting certain conditions summarized below) continue to use Standard Contractual Clauses (SCCs) as a valid mechanism for transferring personal data outside the EEA. The CJEU confirmed that organizations transferring personal data outside the EEA (data exporters) must, in cooperation with the recipients of such personal data (data importers), assess whether there is a level of protection for the personal data transferred that is essentially equivalent to that guaranteed in the EEA by GDPR. Data exporters must carry out these assessments even when data exporters and data importers use SCCs as the basis for the transfer. When transferring personal data uploaded to the AWS services under their AWS accounts (customer data) outside the EEA, customers are data exporters and AWS is the data importer.

In Schrems II, the CJEU also confirmed that, depending on the above assessment, AWS and its customers could need to take "supplementary measures" (in addition to implementing SCCs) to ensure there is an essentially equivalent level of protection for personal data transferred to countries outside the EEA.

Overview of the EDPB Recommendations

The EDPB, a body which includes representatives from data protection authorities of all EU member states, provided examples of supplementary measures in its "[Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#)" (EDPB Recommendations). The EDPB Recommendations also provide guidance for assessing whether there is an essentially equivalent level of protection for data transfers outside the EEA following Schrems II. The EDPB Recommendations recommend that data exporters perform the following six-step data transfer assessment (the EDPB data transfer assessment):

- **Step 1:** Perform a mapping of international data transfers, and assess whether the data transferred is adequate and limited to what is strictly necessary.

- **Step 2:** Verify the transfer tool on which the transfer relies (for example, customers rely on the SCCs to transfer customer data).

- **Step 3:** Assess the laws or practices of the third countries that may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including by using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

- **Step 4:** If the data exporter's assessment is that the use of the transfer tool alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical or organizational measures that are necessary to bring the level of protection of the data transferred up to the EEA standard of essential equivalence.

- **Step 5:** Take any formal procedural steps the adoption of your supplementary measure(s) may require.

- **Step 6:** Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the data exporter transfers to third countries, and monitor if there have been or there will be any developments that may affect it.

Impact of Schrems II and the EDPB Recommendations on the use of AWS services

By their selection and configuration of AWS services, AWS customers control whether or not the AWS services transfer customer data outside the EEA. AWS customers can continue to use AWS services to transfer customer data outside the EEA in compliance with data protection laws (including GDPR). AWS incorporates the AWS GDPR Data Processing Addendum (AWS GDPR DPA) into the AWS Service Terms, which means that the AWS GDPR DPA applies automatically for all customers who use AWS services to process customer data subject to GDPR where AWS is the processor (as defined in GDPR) of this customer data. Furthermore, AWS's highest priority is securing customer data, and AWS implements rigorous technical and organizational measures to protect its confidentiality, integrity, and availability, regardless of which AWS Region the customer has selected. AWS provides advanced encryption services and tools that AWS customers can use to protect customer data. AWS customers can manage their own encryption keys from within a number of native AWS or third-party encryption solutions. AWS follows strict policies when handling disclosure requests from governmental bodies, and makes strong contractual commitments to protect customer data, as set out in further detail in the *Contractual measures* section.

AWS will continue to update its practices to meet the evolving needs and expectations of customers and regulators, and fully comply with all applicable laws in every country in which it operates. For more information, see the Customer update on the EU-US Privacy Shield and the Customer update on strengthened commitments to protect customer data.

Mapping transfers of customer data

This section of the document will help customers address step 1 of the EDPB data transfer assessment.

> **Step 1:** Perform a mapping of international data transfers, and assess whether the data transferred is adequate and limited to what is strictly necessary.
>
> The information provided in this section helps customers to determine whether or not their use of AWS services may require a transfer of customer data to third countries. If, in step 1, the customer determines that its use of AWS services may require a data transfer, the customer can use the information provided in the subsequent sections of this document to learn more about how AWS assists customers to address the EDPB requirements for such data transfer (steps 2 – 6 of the EDPB data transfer assessment).

AWS contracting party

As described in the AWS Customer Agreement, which governs our customers' use of the AWS services, AWS's European seller of record (Amazon Web Services EMEA SARL), based in Luxembourg, is the AWS contracting party that provides AWS services to customers located in Europe, the Middle East and Africa (other than South Africa). In accordance with the AWS Customer Agreement, other AWS affiliates provide the AWS services to customers located outside of Europe, the Middle East and Africa.

How customers can transfer customer data

In accordance with the AWS GDPR DPA, customers select the AWS Region in which they store their customer data. Customers can find an overview of available AWS Regions at the Regions and Availability Zones website. In accordance with the AWS GDPR DPA, AWS will not transfer customer data outside the customer's selected AWS Region unless it is necessary to provide the AWS services initiated by the customer, or as necessary to comply with law or a valid and binding order of a governmental body.

With AWS, customers own their customer data, control its location, and control who has access to it. AWS is transparent about how AWS services process customer data. As set out on the Privacy Features of AWS Services website, each customer can use AWS services with the confidence that customer data stays in the AWS Region that the customer selects. A small number of AWS services involve the transfer of customer data, for example, to develop and improve those AWS services, where customers can opt-out of the transfer, or because transfer is an essential part of the AWS service (such as a content delivery service). AWS prohibits, and its systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by customers, is required to prevent fraud and abuse, or to comply with law.

For more information on AWS's approach to handling requests from governmental bodies, see the *Assessing the laws of the recipient country* and *Supplementary measures* sections.

Validated by the EDPB and approved by the French Data Protection Authority (CNIL), the Cloud Infrastructure Service Providers Europe (CISPE) Data Protection Code of Conduct (CISPE Code) assures organizations that their cloud infrastructure service provider meets the requirements applicable to personal data processed on their behalf (customer data) under GDPR. The CISPE Code goes beyond compliance with GDPR by requiring cloud infrastructure service providers to give customers the choice to use services to store and process customer data exclusively in the EEA. AWS has initially declared 100 services under the CISPE Code and is committed to bringing additional AWS services into the scope of the CISPE compliance program. For further information, see AWS cloud services adhere to CISPE Data Protection Code of Conduct for added GDPR assurance. For more information, see the *Organizational measures* section.

Sub-processing

Customers can determine the processing location for customer data by reviewing the AWS sub-processor website, where AWS lists the subcontractors that it has engaged to provide processing activities on customer data on behalf of the customer (sub-processors).

Sub-processors relevant to an individual customer will depend on the AWS Region the customer selects and the particular AWS services that the customer uses.

There are three types of sub-processors: (1) AWS entities that provide the infrastructure on which the AWS services run; (2) AWS entities that support specific AWS services which may require these entities to process customer data; and (3) third parties that AWS has contracted with to provide processing activities for specific AWS services. The second type of sub-processors includes AWS entities that provide AWS Support services, but these entities do not process customer data unless the customer wants to share customer data in the course of requesting AWS Support (which AWS does neither require nor recommend).

AWS will update the sub-processor website at least 30 days before engaging a new sub-processor, and if customers subscribe for updates, AWS will notify them by email of changes to this website.

Transfer tool

This section of the document will help customers address step 2 of the EDPB data transfer assessment.

> **Step 2:** Verify the transfer tool on which the transfer relies (for example, SCCs).

Where customers instruct the AWS services to transfer customer data to third countries in accordance with the *Mapping transfers of customer data* section, AWS uses the SCCs that the European Commission adopted in June 2021 to validate such transfers, and takes and makes available supplementary measures to protect customer data.

The SCCs are part of the AWS Service Terms and incorporated by reference into the AWS GDPR DPA. They enable all customers that are controllers or processors under GDPR to continue to transfer

customer data in compliance with GDPR. AWS includes the [Controller-to-Processor version of the SCCs](#) and the [Processor-to-Processor version of the SCCs](#) to the AWS GDPR DPA. The Controller-to-Processor clauses apply to transfers of customer data to a third country when the customer is a controller, and the Processor-to-Processor clauses apply to transfers of customer data to a third country where the customer is a processor. See [New Standard Contractual Clauses now part of the AWS GDPR Data Processing Addendum for customers](#) for further information.

Both the Schrems II ruling and the EDPB Recommendations confirm that SCCs are a valid mechanism for transferring personal data subject to GDPR outside the EEA. AWS customers can therefore continue to rely on the SCCs included in the AWS GDPR DPA for transfers of customer data, in compliance with GDPR.

Assessing the laws and practices of the recipient country

This section of the document will help customers perform step 3 of the EDPB data transfer assessment.

> **Step 3:** Assess the laws or practices of the third countries that may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including by using [Recommendations 02/2020 on the European Essential Guarantees for surveillance measures](#).

With AWS, customers are free to select from a suite of on-demand AWS services that customers can provision and configure to build their own products and service offerings. AWS gives customers control over their customer data at all times, through simple, yet powerful, tools that enable them to determine where their customer data will be stored, and to secure their customer data in transit and at rest. Customers are best placed to determine the laws that apply to customer data because they determine how, where and why they process the customer data that they use with the AWS services.

Customers that have questions about US surveillance laws, including the Foreign Intelligence Surveillance Act 1978 (FISA) section 702, can review the [White Paper](#) that the US Department of Commerce, Department of Justice and the Office of the Director of National Intelligence jointly issued in September 2020 detailing the limits and safeguards pertaining to their access to data in response to the Schrems II ruling (the White Paper). The White Paper states that for many companies, the issue of national security access to their personal data is unlikely to arise because this data would not be of interest to national security agencies. The White Paper notes that:

- Companies handling "ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data."

- "The theoretical possibility that a US intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data." The White Paper also notes that such access to data could occur anywhere in the world, not just in the US.

- There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages.

- Additional privacy safeguards have been added to FISA section 702 including amendments made in 2018 that added: (i) querying procedures (in addition to targeting and minimization procedures);(ii) provisions improving oversight by the Privacy and Civil Liberties Oversight Board; (iii) privacy and civil liberties officer requirements to additional relevant agencies; (iv) expanded whistleblower protections to contractors; and (v) transparency requirements including provisions for disclosing the number of FISA section 702 targets.

Irrespective of the laws that apply and regardless of the country from which it originates, AWS reviews every law enforcement request individually and independently. Amazon has a history of formally challenging government requests for customer information that it believes are overbroad or otherwise inappropriate. AWS will continue to thoroughly scrutinize such requests, including those that conflict with local law such as GDPR, and object where it has appropriate grounds to do so. AWS also takes and makes available supplementary measures to support the effectiveness of the SCCs, as described in the *Supplementary measures* section. These supplementary measures include AWS's supplementary addendum to the AWS GDPR DPA in which AWS makes strengthened contractual commitments to challenge law enforcement requests, as set out in further detail in the *Contractual measures* section.

The EDPB Recommendations also permit AWS customers to consider AWS's practical experience "with relevant prior instances of requests for access received from public authorities" outside of the EEA. To help AWS customers assess these prior requests, AWS publishes regular reports on the Amazon Information Requests webpage, about the types and volume of law enforcement requests that AWS receives. The information provided in the Information Request Reports demonstrates that disclosures by AWS of customer data in response to government requests for information are very rare.

So far, no request resulted in disclosure to the U.S. government of enterprise or government content data located outside the United States.

Supplementary measures

This section of the document will help customers perform steps 4, 5 and 6 of the EDPB data transfer assessment.

Step 4: If the laws or practices of the third countries mean that the use of the transfer tool alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical or organizational measures that are necessary to bring the level of protection of the data transferred up to the EEA standard of essential equivalence.

Step 5: Take any formal procedural steps the adoption of your supplementary measure may require.

Step 6: Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the exporter transfers to third countries, and monitor if there have been or there will be any developments that may affect it.

The EDPB Recommendations identify a non-exhaustive list of supplementary measures that AWS and its customers can adopt, depending on the outcome of customers' data transfer assessment described in the *Overview of the EDPB Recommendations* section. These supplementary measures fall into the following three categories: (a) ***technical measures***, such as encryption and logging; (b) ***contractual protections***, including commitments with respect to law enforcement requests for data like those AWS makes in the AWS supplementary addendum; and (c) ***organizational measures***, consisting of internal policies and standards, measures to minimize the collection and retention of data, and adoption of codes of conduct.

This section sets out the key technical, contractual and organizational supplementary measures that AWS takes and makes available to protect customer data and support the effectiveness of the SCCs. AWS will continue to update this document as its supplementary measures evolve.

Technical measures

Customer control

Customers have control over their customer data through simple, yet powerful, AWS services and tools that allow them to determine where customer data will be stored, how it is secured, and who has access.

Shared Responsibility Model

AWS operates a Shared Responsibility Model, which apportions security and compliance responsibilities between AWS and customers based on the way AWS services operate and the degree of control each party has under the AWS services. Under the Shared Responsibility Model, AWS is responsible for providing secure infrastructure and services (Security "OF" the Cloud), while customers are responsible for architecting and securing their applications and solutions that they elect to deploy in the AWS cloud (Security "IN" the Cloud).

For Security of the Cloud, AWS implements responsible and sophisticated technical and physical controls and processes designed to prevent unauthorized access or disclosure of customer data (as evidenced by its compliance program detailed on the AWS compliance website).

For Security in the Cloud, AWS makes available products, tools and services that customers can use to architect and secure their applications and solutions. AWS provides examples of such key products, tools and services in the remainder of this section, and customers can also refer to the AWS Well-Architected website for further information about such products, tools and services.

Encryption

Encryption (including the management of encryption keys) is a key technical supplementary measure described in the EDPB Recommendations. AWS provides advanced encryption services and tools that AWS customers can use to protect customer data. AWS customers can manage their own encryption keys from within a number of native AWS or third-party encryption solutions. AWS Key Management Service (AWS KMS), as a managed service, makes it easy for customers to create and control their encryption keys, and uses FIPS-140-2 certified Hardware Security Modules (HSMs) to protect the security of such keys. All requests to use keys in AWS KMS are logged in AWS CloudTrail so customers can understand who used which key, in what context, and when it was used. Event data logged to AWS CloudTrail cannot be altered. AWS KMS is designed so that neither AWS (including AWS employees) nor third-party providers to AWS have the ability to retrieve, view, or disclose customers' master keys in an unencrypted format.

AWS Nitro System

The AWS Nitro System is the underlying platform for all modern Amazon Elastic Compute Cloud (EC2) instances, and it provides additional confidentiality and privacy for customers' applications. Using purpose-built hardware, firmware, and software, the AWS Nitro System provides unique and industry-leading security and isolation by offloading virtualization functions, like storage and networking, to dedicated hardware and associated firmware. The AWS Nitro System is also designed to have no AWS operator access. With the AWS Nitro System, there's no mechanism for any system or person to log in to EC2 servers (the underlying host infrastructure), read the memory of EC2 instances, or access any data stored on instance storage and encrypted Amazon Elastic Block Store (EBS) volumes.

Contractual measures

AWS GDPR DPA

In the AWS GDPR DPA, AWS makes contractual commitments about the measures it takes and makes available to protect customer data. For example, AWS contractually commits to (i) implement technical measures to protect the AWS network, (ii) assist customers in complying with their security obligations under GDPR by offering tools and functionalities, and (iii) provide third party certifications and audit reports so that customers can verify AWS's compliance with the AWS GDPR DPA.

Supplementary addendum

AWS released a supplementary addendum to the AWS GDPR DPA which sets out contractual commitments that customers can use as supplementary contractual measures in accordance with the EDPB Recommendations. In the supplementary addendum, AWS commits to (i) use every reasonable effort to redirect any governmental body requesting customer data to the applicable customer; (ii) promptly notify the applicable customer about the request if legally permitted to do so; and (iii) challenge any overbroad or inappropriate request, including where the request conflicts with EU law. AWS also commits that if, after exhausting the preceding steps, it remains compelled to disclose customer data, AWS will disclose only the minimum amount of customer data necessary to satisfy the request. To support customers with assessing the laws of recipient countries (see *Assessing the laws of the recipient country*), AWS warrants that it has no reason to believe that the legislation applicable to AWS or its sub-processors, including in any country to which customer data is transferred, prevents AWS from fulfilling its obligations under the AWS GDPR DPA or the supplementary addendum. AWS also commits to promptly notify any change in legislation which is likely to have a substantial impact on AWS fulfilling its obligations. For more information, see AWS and EU data transfers: strengthened commitments to protect customer data.

Organizational measures

Processes

AWS has internal processes to deal with governmental requests for customer data, and irrespective of the source of the request or the laws that apply, AWS reviews every governmental request individually and independently in accordance with its law enforcement guidelines and commitments in the AWS supplementary addendum. AWS rigorously limits – or rejects outright – law enforcement requests for customer data coming from any country, including the United States, where they are overly broad or AWS has any appropriate grounds to.

Information Request Reports

AWS knows that transparency matters to its customers, so AWS regularly publishes on the Amazon Information Requests webpage an Information Request Report (IRR) about the types and volume of governmental requests it receives. Beginning with the July-December 2020 report, AWS launched a new IRR format as an organizational supplementary measure that provides more information about the types of governmental requests AWS receives, and the country of origin of such requests. To use this new IRR format, see the Amazon Information Request Report. The information provided in the IRRs demonstrates that disclosures by AWS of customer data in response to government requests for information are very rare. So far, no request resulted in disclosure to the U.S. government of enterprise or government content data located outside the United States.

Adherence to CISPE Data Protection Code of Conduct

Validated by the EDPB and approved by the CNIL, the CISPE Code assures organizations that their cloud infrastructure service provider meets the requirements applicable to personal data processed on their behalf (customer data) under GDPR. The CISPE Code goes beyond compliance with GDPR by requiring cloud infrastructure service providers to give customers the choice to use services to store and process customer data exclusively in the EEA. AWS initially declared 100 services under the CISPE Code because of the added assurance that it provides to AWS customers that AWS has implemented contractual and operational measures that meet the requirements applicable to a processor under Article 28 of GDPR. AWS compliance with the CISPE Code has been verified by EY CertifyPoint, an external auditor accredited by the CNIL as a monitoring body. AWS customers can access a list of the 100 AWS services that are verified as compliant with the CISPE Code on the CISPE Public Register. AWS is committed to bringing additional AWS services into the scope of the CISPE compliance program based on customer feedback and completing the intensive verification process with EY CertifyPoint for declaring further AWS services.

For further information, see AWS cloud services adhere to CISPE Data Protection Code of Conduct for added GDPR assurance.

Additional resources

To help customers further understand how they can address their 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.

Document history

Date	Description
September 2021	First publication
January 2023	Updated version