Data Protection in the Cloud

Guidance for Public Sector Bodies in Ireland

Contents

1. Protecting data in the cloud

Many public sector bodies (PSBs) in Ireland use the AWS Cloud to digitally transform services and better serve citizens. Government authorities such as the National Cyber Security Centre (NCSC) and the Data Protection Commission (DPC) acknowledged this transformation by releasing the Guidance for Organisations Engaging Cloud Service Providers (DPC Guidance). This guidance advises PSBs on how to protect their most critical and sensitive assets—their data.

With over a decade of experience working with public sector customers in more than 190 countries and territories, AWS is committed to continuously raising the bar on protection safeguards and services. Read on for support in planning AWS Cloud deployments that meet data protection requirements and see how to align with government security considerations.

1.1. The AWS cloud

DPC Guidance advises that with an increasing number of cloud services, PSBs should ensure there is adequate security for processing personal data. AWS shares security and compliance responsibilities with PSBs. This shared responsibility model can help relieve the operational burden of PSBs, since AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. It's a PSB's responsibility to classify its data and implement the appropriate controls within its AWS Cloud environment. By using AWS services, PSBs can architect to meet its data protection requirements.

> "We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching encryption auditing and logging, entitlement and compliance."
>
> **John Brady**
> CISO, Financial Industry Regulatory Authority (FINRA), US

As shown in Figure 1, this differentiation of responsibility is commonly referred to as security of vs. in the cloud.

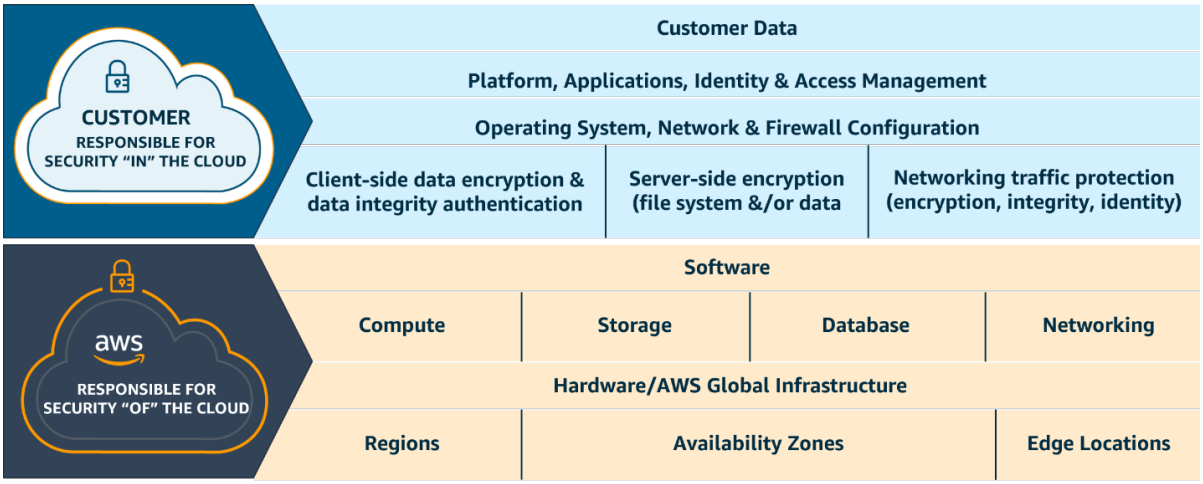

Figure 1. The AWS Shared Responsibility Model

1.2. Data processors and data controllers explained

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

As a data processor. When PSBs use AWS services to process personal data in the content they upload to AWS services, AWS acts as a data processor. PSBs can use the controls available in AWS services, including security configuration controls, for handling personal data. The PSB may act as a data controller or processor itself, and AWS acts as a data processor or sub-processor.

As a data controller. When AWS collects personal data and determines the purposes and means of processing that personal data—for example, when AWS stores contact information for the AWS account to aid through customer support activities—it acts as a data controller.

2. Control over data location and data transfers

AWS enables PSBs to comply with data location and transfer considerations presented in DPC Guidance, as PSBs retain control of their personal data and determine where their personal data will be stored, including the geographic region of that storage. PSBs choose the AWS Regions in which to store their data. They deploy AWS services only in the locations of choice, in accordance with specific geographic requirements. For example, PSBs in Ireland can store data in the AWS Ireland Region while still using multiple Availability Zones to develop highly scalable, available, and fault-tolerant applications that can adhere to data residency and sovereignty requirements.

AWS will not move or replicate PSB data from the selected AWS Regions unless to comply with law, for the provision of a service that is not regional, or because transfer is an essential part of the service (such as a content delivery service, or others found here). If the service terms specify an exception, such as to develop and improve those services, PSBs are able to opt-out of transfers of customer data (such as the services found, here).

"Our data is hosted in Europe, which is crucial for us from a security perspective. With AWS, we have complete control over where and how data is stored and who has access to it. This control along with the extensive encryption, means we feel safe. We know the Trust's data is protected."

Martin Brambley
Director of Managed Service Provider Sirocco Systems, National Trust, UK

2.1. GDPR Compliance When Using AWS Services

DPC Guidance recognises the increasing number of cloud services and the importance of ensuring adequate security for personal data being processed by the PSBs that use them. PSBs can use all AWS services to process personal data in compliance with the GDPR. All generally available AWS services and features adhere to the high privacy bar and data protection standards required of data processors by the GDPR. This means that in addition to benefiting from all of the measures that AWS already takes to maintain the security of services, PSBs can deploy AWS services as part of their GDPR compliance plans. The AWS GDPR Data Processing Addendum (AWS GDPR DPA) is incorporated into the AWS Service Terms and applies automatically to all customers, enabling PSBs to comply with GDPR.

Wellola, an Irish digital health software firm, believes that the future of healthcare is preventative, community-based, and supported by digital tools. Using AWS, Wellola scaled quickly to meet demand caused by a spike in users when the COVID-19 pandemic began. They delivered a reliable, secure, and cost-effective platform that met regulatory standards and HIPAA and GDPR requirements.

"In healthcare, data protection and governance are the most important thing of all, so we use AWS Identity and Access Management (IAM) and AWS Organizations to provide access to features to internal and third-party developers. It just makes life a lot safer."

Chris O'Codlatain Lachtna
CTO and Co-Founder, Wellola, Ireland

Corresponding with DPC Guidance, PSBs can use AWS services to transfer personal data from the European Economic Area (EEA) to non-EEA countries that have not received an adequacy decision from the European Commission in compliance with the GDPR. The Court of Justice of the European Union (CJEU) issued a ruling that validated the use of Standard Contractual Clauses (SCCs) as a mechanism for transferring customer data outside the EEA. AWS customers can continue to rely on the SCCs included in the AWS GDPR DPA if they choose to transfer their data outside the EEA in compliance with the GDPR.

PSBs will need to perform a Transfer Impact Assessment if they choose to use a non-regional service or a region outside of EEA. PSBs can use the Privacy Features for AWS Services page to determine whether their use of an individual AWS service involves the transfer of customer data and ether opt out or implement supplemental measures.

The AWS whitepaper, Navigating Compliance with EU Data Transfer Requirements, provides information about the services and resources that can help PSBs conduct data transfer assessments in light of recent CJEU rulings and subsequent recommendations from the European Data Protection Board (EDPB).

AWS offers strengthened contractual commitments that go beyond what is required by the recent CJEU rulings and currently provided by other cloud service providers (CSP) to protect the personal data that PSBs trust AWS to process. Significantly, these new commitments apply to all customer data processed by AWS that is subject to GDPR, whether it is transferred outside the EEA or not. These commitments are automatically applicable to all PSBs using AWS to process their personal data, through the supplementary addendum to the AWS GDPR DPA.

AWS is committed to important EU privacy, portability, and digital sovereignty programmes—including the SWIPO infrastructure as a service (IaaS) Code of Conduct, GAIA-X, and CISPE Data Protection Code of Conduct (CISPE Code). AWS adherence to the CISPE Code gives PSBs additional assurances that AWS implemented contractual and operational measures that meet the requirements applicable to a processor, under Article 28 of the GDPR. AWS's compliance with the CISPE Code has been verified by EY CertifyPoint, an external auditor accredited by the French Data Protection Authority (CNIL), acting as the lead data protection authority.

For more information on how AWS can enable GDPR compliance, refer to the AWS GDPR Center, the GDPR FAQs, and the following resources: How AWS is helping EU customers navigate the new normal for data protection; and Using AWS in the context of Common Privacy and Data Protection Considerations.

For a list of AWS services that can help you navigate GDPR compliance, refer to the Navigating GDPR Compliance on AWS whitepaper.

3. Explaining security considerations

"As a healthcare technology vendor, data security is at the core of everything we do. AWS governance controls have made it easy for us to invest heavily in security and to safeguard the integrity of healthcare data. Configurable layers of encryption, jurisdictional data control, and access management has allowed us to remain aligned with local, national, and international compliance standards such as the National Health Service (NHS) data protection, EU General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPPA), etc."

Jonathan Larbey
CEO, T-Pro, Ireland

DPC Guidance explains that PSBs that entrust personal data to a CSP must be satisfied that the CSP's security standards are sufficient and appropriate for the processing of personal data undertaken on the PSB's behalf.

At AWS, security is our top priority. As AWS is both a data processor and a data controller under GDPR, AWS implements responsible and sophisticated technical and physical controls and processes designed to prevent unauthorised access or disclosure of PSBs' data (see Data Protection at AWS). To determine what tools PSBs might need to meet compliance needs, we continually monitor the evolving privacy regulatory and legislative landscape to identify changes (see Data Privacy FAQ).

We aim to earn PSB trust by simplifying the challenges usually associated with activities surrounding data protection. For example, to comply with the GDPR, PSBs may need to conduct a Data Protection Impact Assessment (DPIA) for processing activities. AWS Marketplace offers a range of security solutions that combine privacy expertise and machine learning (ML) to simplify this process and help mitigate risk. For further guidance, including templates, PSBs can refer to the GDPR.EU: How to conduct a Data Protection Impact Assessment website.

AWS supports more security standards and compliance certifications than any other offering, helping to satisfy compliance requirements for virtually every regulatory agency around the globe. PSBs inherit these with the AWS services they use, reducing their compliance workload. We offer guidance to maintain compliance, and we offer a large network of AWS Partners who can help manage compliance on behalf of a PSB—if desired.

3.1. How to protect your data

PSBs retain full control of their data and determine who can access it. We provide the most comprehensive set of services, tooling, and expertise to help protect PSB data. AWS can help PSBs improve their ability to meet core security and data protection requirements by aligning with DPC Guidance and wider government advice in the following areas.

Identification
View the Data Classification Overview to learn how to classify data to evaluate sensitivity and business impact, assess risks associated with different types of data, and determine appropriate protection. Use tools like Amazon Macie, which uses ML to automatically recognise sensitive data, such as personally identifiable information (PII) or intellectual property, and provides dashboards and alerts that give visibility into how this data is being accessed or moved.

Pseudonymisation and encryption
Encrypt data to reduce the risks associated with the storage and processing of personal data. AWS provides data encryption capabilities for over 100 services and provides blog posts to highlight the importance of encryption and how AWS can help. Use cryptographic key storage like AWS Key Management Service (AWS KMS) to generate and manage both root keys and data keys. Implement encryption and decryption operations on all types of data in a client-side encryption library with AWS Encryption SDK. Use services such Amazon Athena to anonymise datasets and tokenisation to replace sensitive data.

Tenant isolation
AWS provides logical separation capabilities and its architecture is designed to isolate each customer from other customers (refer to Logical Separation on AWS whitepaper). Use features like AWS Nitro Enclaves to create isolated compute environments to further protect and securely process highly sensitive data such as PII, healthcare, financial, and intellectual property data within their Amazon Elastic Compute Cloud (Amazon EC2) instances. Use Amazon Virtual Private Cloud (Amazon VPC) to launch AWS resources in a logically isolated virtual network that you can define. Provision dedicated hypervisor-enabled or bare-metal

Technical and organisational measures

Architect for confidentiality, integrity, and availability of personal data by building secure applications. Manage access to AWS services and resources securely with IAM. You can create and manage AWS users and groups as well as use permissions to allow and deny access to AWS resources. Use AWS CloudTrail to log, continuously monitor, and retain information about account activity related to actions in AWS, which simplifies security analysis, resource change tracking, and troubleshooting. Use Amazon GuardDuty, a managed threat detection service, to continuously monitor for malicious or unauthorised behaviour to help protect AWS accounts and workloads.

Backup and restore

Use AWS Backup to automate and centrally deploy data protection policies to configure, manage, and govern your backup activity. Use AWS Elastic Disaster Recovery (AWS DRS) to minimise downtime and data loss with fast, reliable recovery. Additionally, Amazon Simple Storage Service (Amazon S3) offers cross-Region replication to replicate data in other AWS Regions for compliance, security, and disaster recovery.

Testing and evaluation

Perform vulnerability scans and security assessments such as penetration tests on your infrastructure. Use services like AWS Config to record and evaluate configurations in your resources, AWS Security Hub for unified security and compliance, and AWS Audit Manager to continuously audit your AWS usage to simplify how you assess risk. We developed a security assurance programme that uses best practices for global privacy and data protection to help you operate securely within AWS. These security protections and control processes are independently validated by multiple third-party independent assessments and can be reviewed on the AWS Compliance page.

Data breaches

PSBs retain the responsibility to monitor their own environment for privacy breaches. Use monitoring tools like Amazon CloudWatch to track when data is accessed and by whom. Use the AWS Security Incident Response Guide to implement a security incident response procedure to plan for security incidents and ensure staff understand how to react to security issues. Report breaches via our Vulnerability Reporting webpage. Subscribe to the AWS Security Bulletins RSS feed to keep abreast of security announcements and the AWS Service Health Dashboard to alert you to any broadly impacting availability issues. Review the Best Practices for Security, Identity, & Compliance page for additional information on how to protect against and detect security breaches.

Data deletion

PSBs control the deletion of their data on AWS, as well as maintaining appropriate data retention policies and procedures. We provide service-specific instructions on how you can delete your system data on the Privacy Features of AWS Services page. For erroneous deletion, AWS services such as Amazon S3, support features that help maintain data version control, prevent accidental deletions, and replicate data to the same or different AWS Region.

Onsite inspections

Instead of allowing PSBs to perform physical audits, AWS has an independent third-party perform audits of its data centres. The auditors produce a SOC 1, Type 2 Report in connection with the audit. Independent reviews of data centre physical security are also part of an ISO 27001 audit, a Payment Card Industry (PCI) Data Security Standard (DSS) assessment, and an International Traffic in Arms Regulations (ITAR) audit.

4. Transparency over data processing

Transparency over data processing is heavily promoted by DPC Guidance. We are transparent about how AWS services process the personal data that PSBs may upload into their AWS accounts, and we provide capabilities that allow PSBs to delete their data and monitor its processing.

> "When you're in telehealth, and you touch protected health information, security is paramount. AWS is absolutely critical to do what we do today. Security and compliance are table stakes. If you don't have those, the rest doesn't matter"
>
> **Cory Costley**
> Chief Product Office, Avizia, US

AWS will only process PSB data under their documented instructions and will not access, use, or share PSB content without agreement, as described in the AWS Customer Agreement and AWS GDPR DPA. We offer sources online to support PSBs with data protection obligations, such as the Data Privacy Centre page and the Privacy Features of AWS Services page. Our online Privacy Notice describes how we collect and use personal information in relation to AWS websites, applications, products, services, and events.

Our strengthened commitments to PSBs build on our long track record of challenging law enforcement requests. If we receive a law enforcement request for personal data from government bodies, whether inside or outside the EEA, we commit to challenge requests that are overbroad, or where we have appropriate grounds to do so, including where the request conflicts with EU law, as described in our supplementary addendum to the AWS GDPR DPA.

We disclose only the minimum amount of customer data necessary to satisfy the request, and provide a bi-annual Information Request Report describing the types and number of information requests AWS receives from law enforcement.

We maintain the AWS Sub-processors page to provide a list of sub-processors that AWS has engaged to provide processing activities on PSB data—on behalf of the PSB. Sub-processors are subject to the same contractual obligations as AWS has under GDPR DPA.

We provide a wide variety of best practice documents, training, and guidance that PSBs can use to protect their data, exemplified by the security pillar of the AWS Well-Architected Framework.

DPC Guidance acknowledges that CSPs—as processors—can use approved codes of conduct or certification mechanisms to demonstrate the compliance of elements of their processing. To validate our alignment with data protection and privacy standards, AWS is assessed by third-party, independent auditors resulting in certifications, audit reports, or attestations of compliance, which can be viewed in AWS Artifact. Standards we comply with include ISO 9001, ISO 27001, ISO 27701, ISO 27018; SOC 1, SOC 2, SOC 3; Health Insurance Portability and Accountability Act (HIPAA); Cloud Infrastructure Services Providers in Europe (CISPE); General Data Protection Regulation (GDPR); Cloud Computing Compliance Controls Catalog (C5); and EU-US Privacy Shield. For the full list, view our AWS Compliance Programs page.

5. Contract considerations

"In the beginning of our journey to the cloud, security and privacy concerns were very present with our clients, but we managed to work our way out with the regulators and we implemented a secure cloud framework with specific cloud controls to really make sure that the cloud was secure. For us, there's no doubt the cloud is secure, but you also have to configure it correctly. You have to make sure the policies and laws of the Flemish Region are being addressed. So, once we got that right, we saw an uptake in revenue and we saw clients really adopting it. We can say that security helps us move faster in the public cloud."

Stefan De Smet,
CIO, IT Shared Service Center of the Flemish Government, Belgium

As stated by DPC Guidance and as the GDPR requires, data processing should be governed by a contract and controllers should retain control over personal data with clear and agreed limitations and obligations.

AWS enables PSBs to align with these considerations as we make several contractual commitments that are reflected in the AWS GDPR DPA and the Supplementary Addendum concerning data location; both the technical organisational measures implemented by AWS and those chosen by the PSB; measures to protect PSB data and notification of data disclosure requests; obligations under the AWS GDPR DPA in compliance with legislation applicable in a third country in which PSBs data is processed; and the statutory rights of individuals in case of violation under GDPR.

AWS may use sub-processors to assist with the processing of customer data or to provide services on our behalf. In alignment with DPC Guidance, all engagements with sub-processors are in accordance with the AWS GDPR DPA. Sub-processors relevant to PSBs will depend on the AWS Region that PSB has selected and the particular AWS services that PSB uses. AWS will update the AWS Sub-Processor page at least 30 days before engaging a new sub-processor, and if PSBs subscribe for updates, AWS will notify them by email of changes to this page.

6. Summary

With the AWS Cloud, PSBs can meet the high levels of protection set by the GDPR. We work closely with PSBs to understand their data protection needs and offer the most comprehensive set of services, tooling, and expertise to help protect PSB data. Our industry-leading privacy safeguards and security controls enable PSBs to operate with the confidence that compliance requirements presented in the DPC Guidance can be achieved.

If you would like to learn more about how AWS can help protect and secure your data in the cloud, please contact the Irish AWS Public Sector team via aws-publicsector-ireland@amazon.com.

Additional resources

General

- Adopting Cloud Technology: Guidance for public sector organisations in Ireland
- Procuring Cloud Technology: Guidance for public sector organisations in Ireland
- Enabling Cloud-Driven Digitalisation: Guidance for public sector organisations in Ireland
- 12 Steps to Cyber Security: Guidance on Cyber Security for Irish Business, NCSC, Government of Ireland
- Five Steps to Secure Cloud-based Environments,Data Protection Commission
- Guidance Note: Guidance for Controllers on Data Security, Data Protection Commission
- Using AWS in the Context of Common Privacy and Data Protection Considerations
- Privacy Features of AWS Services
- Data Protection at AWS

GDPR

- General Data Protection Regulation (GDPR) Center
- Navigating GDPR Compliance on AWS
- AWS and the General Data Protection Regulation (GDPR)
- Customer update: AWS and the EU-US Privacy Shield
- AWS and EU data transfers: strengthened commitments to protect customer data
- AWS GDPR Data Processing Addendum—Now Part of Service Terms
- Protecting data is our ongoing commitment to EU customers

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.