Customer data in aws

Azets Insight AS

22. April, 2021

v1.0

AZETS

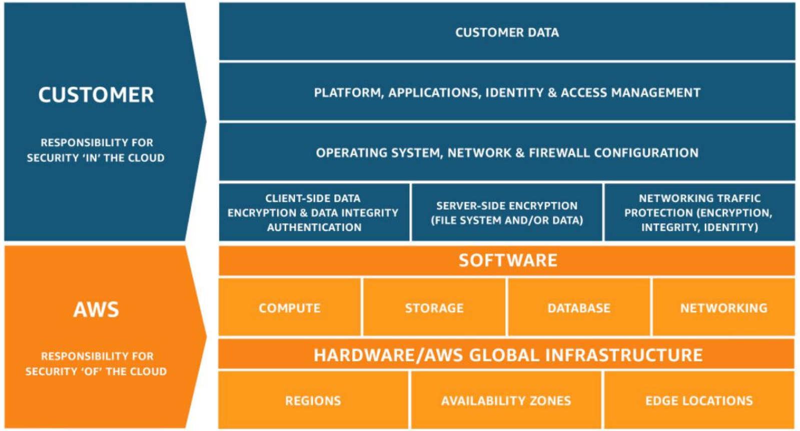
Introduction

Amazon Web Services (AWS)
Azets use Amazon Web Services (AWS) as a public cloud service provider. For data privacy and compliance reasons, Azets is using the AWS Stockholm region for data storage and compute. The AWS Stockholm region consists of three different data centers located around Stockholm, Sweden.

Shared Responsibility Model
AWS provides a Shared Responsibility Model. This means that AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.
In this model, Azets is responsible for the design, implementation and maintenance of the systems that holds and process Azets data and customer data, including making sure that the data is sufficiently secured both in transit and at rest. This means only Azets have access to the environment Azets maintains in AWS.

Appendix
To give a better understanding of how Azets protects data stored in the AWS environment, this report includes detailed descriptions on the following topics:

- Access to data
- Securing of data
- Compliance
- Data storage according to Norwegian legislation
- AWS Certification
- Azets Security Organization



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Access to data

Physical access to data centers
Like all AWS data center locations, the Stockholm AWS locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Emergency power, HVAC cooling, advanced fire protection and physical security measures are implemented in all AWS data centers. AWS data center physical locations are a well-kept secret, and only a small group of AWS technical and security personnel are allowed on the premises. Security measures include (but are not limited to) 24/7 surveillance, on-site security guards, perimeter fences, mantraps and secure access control.

Data center redundancy
To prohibit the loss of availability in case access to one data center it lost, Availability Zones are built to be independent and physically separated from one another. Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS Customer Agreement
In accordance with the AWS Customer Agreement signed by Azets and AWS, Azets can never lose permanent access to any data Azets stores in AWS. Even in a breach of terms or dispute situation, access would only be temporary suspended.
This agreement is available from the AWS website.

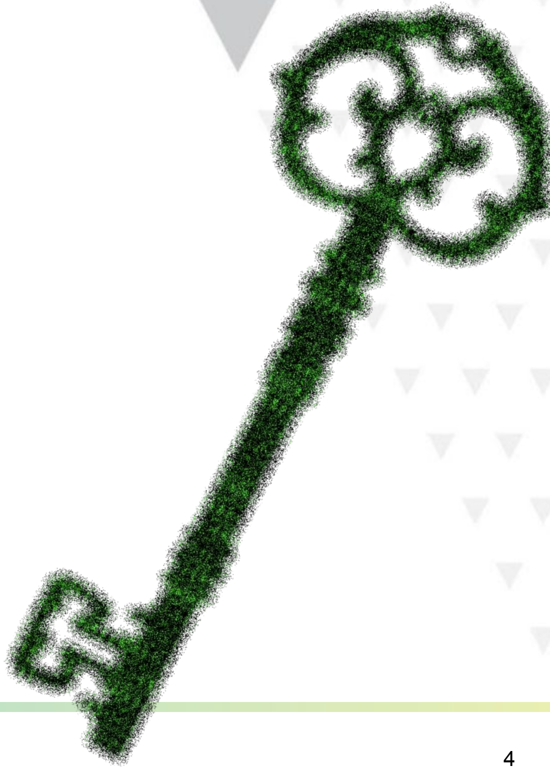
Securing of data

Secure access
Access to the Azets AWS environment are controlled by strict access management procedures, and only Azets personnel have access to the environment. All personal access also requires personal accounts with the correct privileges, and access is only possible using multi-factor authentication. Azets policies sets strict requirements for the handling and construction of passwords. Access management is controlled by policy and accesses are audited twice a year. To ensure that there is a healthy security culture in Azets, all personnel must participate in mandatory security awareness training presented regularly by the security team.

Malware protection and security monitoring
All server instances key components of the infrastructure, such as Active Directory or File Servers, are protected with advanced malware detection and prevention solutions. Security patching is performed using local WSUS and AWS System Manager, and the environment is scanned periodically for vulnerabilities with AWS Inspector.
Services such as AWS GuardDuty and Sentinel One are used for security monitoring for the key aspects of the infrastructure. Sentinel One is an AI-driven security monitoring and antivirus software. Datadog, Zabbix, AWS Inspector and AWS Security Hub are also used to identify security events and monitor vulnerabilities. In the case of a security incident, all relevant technical personnel is automatically alerted.

Data encryption
Azets are using AWS KMS to encrypt data at rest for native AWS storage, and to protect other keys that are distributed to applications which directly encrypt data. AWS KMS is using AES-256 and it is validated under the National Institute of Standards and Technology's FIPS 140-2 program, the standard for evaluating cryptographic modules. Encryption using a FIPS 140-2 validated cryptographic module is often a requirement for other security-related compliance schemes like FedRamp and HIPAA-HITECH in the U.S., or the international payment card industry standard (PCI-DSS). All storage that contains customer data and/or sensitive data is encrypted, including all backups.

For AWS managed services such as (but not limited to) AWS S3 and AWS Managed database offerings, data in transit are protected via SSL/TLS using AWS proprietary implementation of TLS called s2n (signal to noise). This overcomes existing problems with other TLS implementations such as OpenSSL. In general, Azets encrypt data at rest and in transit for all Azets managed storage in AWS.



Compliance

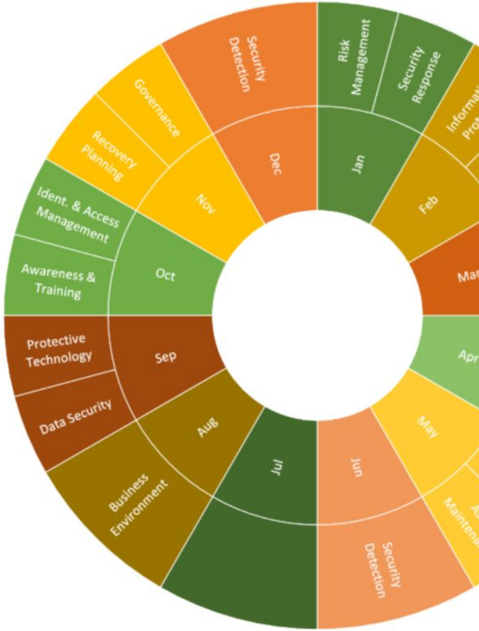
Risk management
To enable a good balance of correct measures applied and efficient use of resources, Azets uses a risk-based approach to information security. This involves using risk-based methods to evaluate vulnerabilities and identify the best measures based on existing threats and likelihood. Azets regularly identifies where risk assessments are needed. This could be both new and existing data processing applications, platforms, physical infrastructure or processes.

Azets uses a yearly risk-wheel stating which activities that must be performed during the year to evaluate and mitigate IT-risk. Identification and evaluation of risks are based on standard risk evaluation methods defined in ISO 31000: 2009.

Privacy
When Azets contracts with service providers (processors) that are ultimately US-owned, we ensure that our contracts are with their UK or EU entities, subject to UK GDPR and EU GDPR legislation respectively. Azets only use data center locations inside the EU/EEA, and make sure that no remote access from third-countries are done for support (or other) purposes.

Azets have risk-assessed the continued usage of such US-owned service providers in compliance with the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. We continually keep under review the requirements which are imposed by applicable legislation.

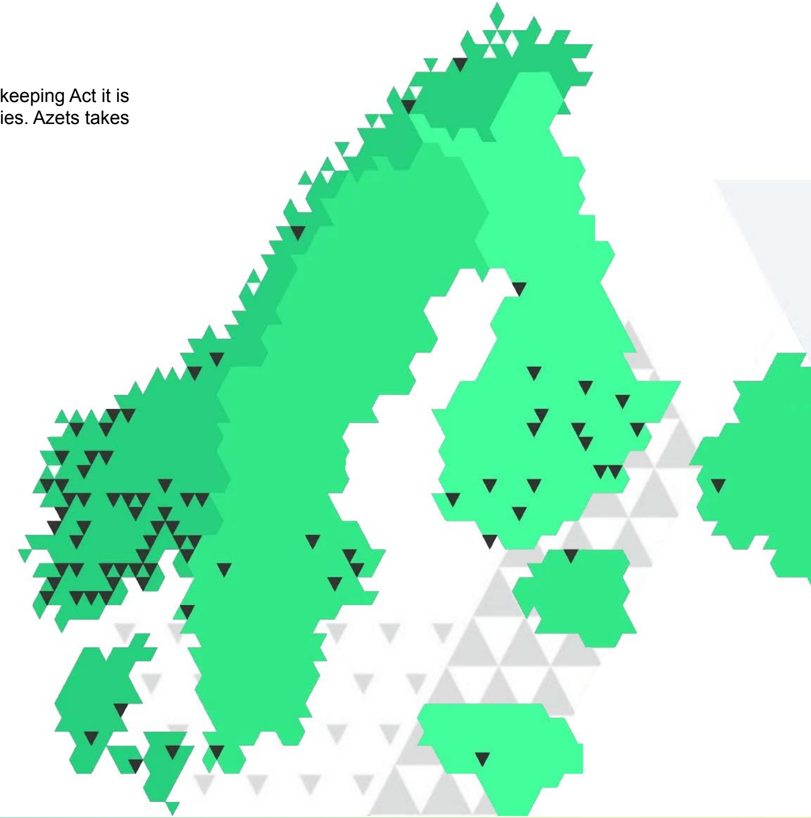
Amazon Web Services has provided a supplementary addendum to the Data Processing Agreement that Azets have with them, which sets out how AWS deal with valid and binding requests from governmental bodies regarding disclosure of customer data. In the unlikely event that Azets shall receive such a request, Azets will notify the data controller and decline the request on the basis that we act as a data processor, and are according to EU GDPR only able to act on the data controllers explicit instructions.



Data storage according to Norwegian legislation

Accounting information stored outside Norway
Azets use the AWS data centers located in Stockholm, Sweden. Following the regulations related to the Norwegian Bookkeeping Act it is allowed to keep Norwegian accounting information stored in Sweden. The only requirement is a notice to the Tax authorities. Azets takes care of these notices.

Relevant legal documents (in Norwegian only):
Lov om bokføring § 13
Forskrift om bokføring § 7-5
Forskrift om oppbevaring av elektronisk regnskapsmateriale i andre EØS-land § 1
Prinsipputtalelse Skatteetaten



AWS Certification

Services in scope
The scope for these certifications cover the service AWS provides in the shared responsibility model. This includes the hardware and infrastructure, AWS software services and AWS data storage services. In cases where Azets manage our own services on the AWS platform, the actual operation of these are not within scope. However, the environment and platform are.
A full list of AWS Services in scope by compliance program is available on the AWS website.

SOC certifications
To demonstrate how AWS achieves key compliance controls and objectives, several independent third-party examinations are performed each year and presented in System and Organization Controls (SOC) reports.
The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance.
AWS supports more security standards and compliance certifications than most other vendors, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

- AWS SOC 1 Report, available from AWS Artifact
- AWS SOC 2 Security, Availability & Confidentiality Report, available from AWS Artifact
- AWS SOC 2 Privacy Type I Report, available from AWS Artifact
- AWS SOC 3 Security, Availability & Confidentiality Report, available as a whitepaper

Access to the reports must be acquired from AWS Artifact by each customer, Azets are contractually prohibited from distributing these reports on behalf of AWS. More details on what information the AWS SOC reports provide can be found here
The SOC reports are performed by Ernst & Young LLP.

ISO certifications
AWS also holds a number of ISO certifications: ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015.

Security organization

Information Security Management System (ISMS)
Azets' business is based on information and data, and as such is dependent on the trust of customers, partners, suppliers and employees. In order to maintain information security at all levels in the organization, and to protect all information assets managed by Azets from threats, whether internal or external, deliberate or accidental, Azets maintains a common Information Security Policy applicable to all parts of Azets. This policy applies to all companies, employees, contractors, consultants, temporaries and other workers in the Azets group. Azets uses established frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Center for Internet Security (CIS) Security Controls and Information Technology Infrastructure Library (ITIL) as reference for IT service management and best practices.

Information Security Governance
Azets Information Security Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated. Governance ensures that security strategies are aligned with business objectives and consistent with regulations. Governance is done at Azets Group level. The main responsibility for Information Security Governance lies with the Chief Information Security Officer (CISO). Each Azets division has a Regional Security Officer (RSO) with responsibilities for local Information Security. The group has regular meetings (Azets Security Forum) lead by the CISO. The meetings address both governance and management related issues.

Security incidents and operations
Azets has established an internal SOC with members from different departments in all countries. Security events reported to the Security Incident Response Team (SIRT) are automatically generated as a ticket in our common ticketing system, and relevant SIRT members are automatically alerted. Tickets are then dispatched to the correct agent. Security events are automatically collected from internal sources like antivirus systems, external SOC services and partners, by direct email to the SIRT team and other relevant sources.

Additional resources

More information about how Azets handles privacy and security can be found in the Azets Trust Center.

For other questions, please call our international sales team on +47 40 10 40 18 to speak with one of our specialists, or contact us on one of the following email addresses:

Norway: kundesenter.no@azets.com
Denmark: info-dk@azets.com
Finland: etunimi.sukunimi@azets.com
UK: hello@azets.co.uk