Midaxo

Midaxo Cloud Security Whitepaper

Version 2024-06

Classification: Public

Executive Summary

Midaxo is committed to maintaining a high level of information security, and its key priority is always protecting customers' information and carefully maintaining the information security of Midaxo Platforms. This Security White Paper gives an overview of the Midaxo Cloud security features.

The certified Midaxo information security management system (Midaxo ISMS) complies with the international ISO/IEC 27001:2013 standard. The design of security controls is based on risk analysis. Risk management is periodically performed throughout the organization to ensure the mitigation of any emerging security risks. Midaxo ISMS defines the security processes, roles, and responsibilities for implementing information security management as an integral part of Midaxo's business and operations. Midaxo ISMS, together with Midaxo's information security policy, are periodically reviewed to ensure they are up to date.

Midaxo Cloud is developed, operated, and maintained by motivated, competent personnel that are committed to maintaining a high level of information security. Continuous security education and training supports them to maintain security awareness in the organization. The technical implementation of Midaxo Cloud has been designed to meet customers' strict security requirements and industry best practices.

Technical security starts with comprehensive security architecture that defines a solid and secure foundation for Midaxo Cloud. The architecture is based on well-proven and widely used secure services, methods, and protocols, and it has been defined to protect data both in transit and at rest and to ensure its confidentiality, integrity, and availability. Strict access control allows only authorized users to access the data.

Operation and maintenance of the Midaxo Cloud follows documented processes and plans. Continuous monitoring of information security and system performance ensures that all deviations and incidents can be responded to in a timely manner by trained and competent personnel in accordance with the incident response process.

Because of today's ever-changing risks and security threats, Midaxo's security team closely monitors security updates, alerts, and advisories from applicable system and software vendors as well as various security organizations and authorities. Based on risk analysis, the security team deploys applicable mitigation methods and security controls. Periodic security audits and technical tests performed by independent third-party information security companies ensure that information security fulfils all requirements and meets the highest standards.

Table of Contents

Introduction to Midaxo Cloud

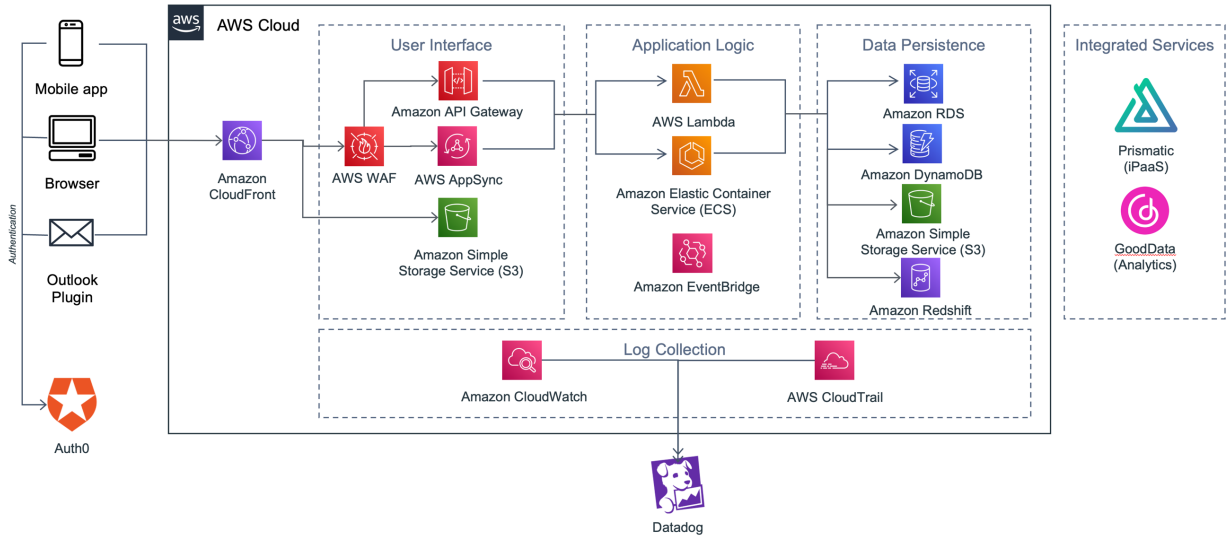
Midaxo Cloud helps Corporate Development teams to perform their business processes, such as mergers and acquisitions (M&A), divestments, various rationalization processes and partnership models in a defined a systematic way.

Midaxo Cloud provides an enterprise-wide workspace, where different business processes and their projects can be managed efficiently.

The Midaxo Cloud is designed for managing confidential information. Therefore, it has multi-level access rights management capabilities, and, by default, users cannot view any projects. Administrative users can grant access to the different processes and individual projects. In addition, within projects, administrative users have granular permissions management options to grant users access only to individual tasks.

Midaxo Cloud Architecture

Midaxo Cloud runs on Amazon Web Services' (AWS) leading cloud platform, utilizing the AWS Serverless Computing. With serverless computing, infrastructure management tasks like capacity provisioning and patching are handled by AWS.



Midaxo Cloud environment contains several distinct layers of services

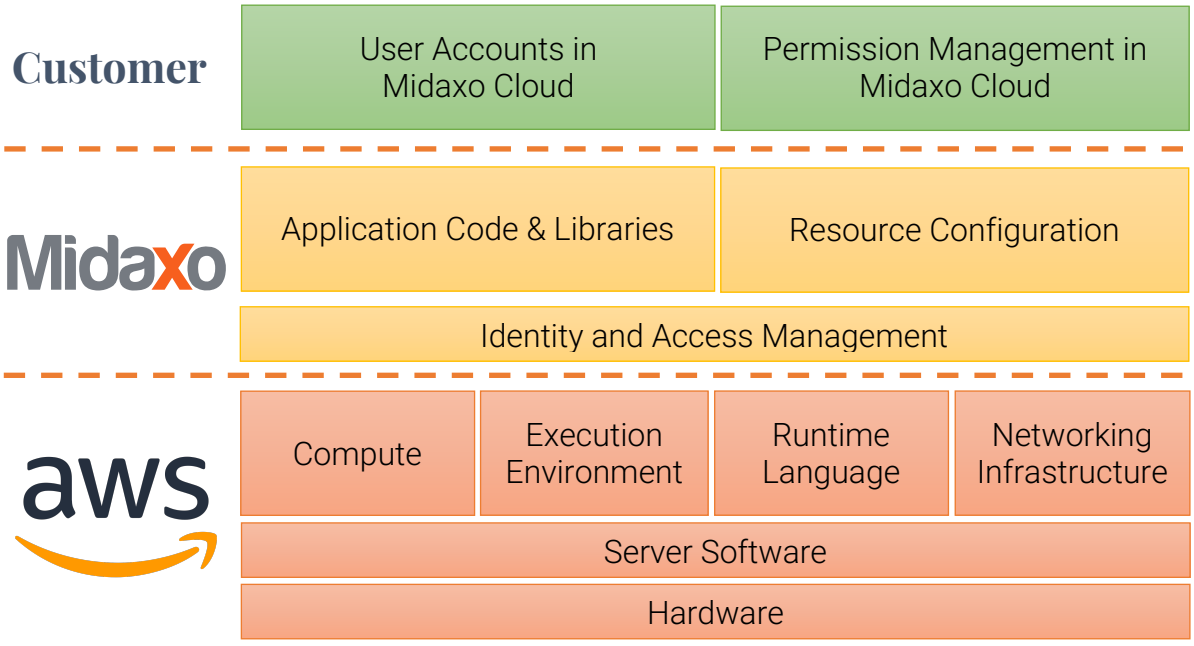
Layer	Description
User Interface layer	Provides the user interface through a Single Page Application (SPA) hosted from Amazon Simple Storage Service (S3). The same User Interface layer is used across all end user clients, such as the browser, mobile app or Outlook plugin.
Authentication layer	Provides authentication for all users through Auth0 identity provider by granting OpenID Connect (OIDC) based short-lived identity and access tokens.
Application Programming Interface (API) layer	Provides the business logic interface for the User Interface layer and is responsible for storing the data to the Data Persistence layer.
Data Persistence layer	Provides the data storage for the Application Interface layer.

Event & Log Handling layer	Provides event handling on user and system activities, triggered by the API and Data Persistence layers.
3rd Party Integrations layer	Provides integrations to 3rd services, such as Good Data analytics and Prismatic iPaaS. Through Prismatic customers can integrate to their own systems, such as Salesforce or Microsoft 365. These integrations are optional and are not enabled by default.

Shared Responsibility model

In serverless computing, Security and Compliance is shared responsibility between AWS and Midaxo. Midaxo is responsible for the security of the actual Application Code and Libraries, AWS Resource Configuration, and for Identity and Access Management.

Customers are responsible for managing the access to Midaxo Cloud, including user accounts and permission management.



More information: https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-lambda/the-shared-responsibility-model.html

Software

Midaxo Cloud is built on top of AWS managed services and is fully Serverless (Midaxo is not managing any virtual machines or physical servers).

User Interface layer hosts a React based Single Page Application (SPA) that embeds other SPAs in the main Single Page Application. This application is hosted on Amazon S3 as a static site and has an Amazon CloudFront content distribution network (CDN) provisioned in front of it.

Authentication layer is fully managed by Auth0 and is integrated to the User Interface layer through Auth0's SDKs and the API layer is configured to trust only tokens issued from the Midaxo Cloud's Auth0 tenant.

API layer has an AWS AppSync GraphQL endpoint provisioned that use AWS Lambda based functions to read and write from the Data Persistence layer. AWS Lambda functions are implemented in Python programming language. API layer publishes events to Amazon EventBridge for communication across the different services within the API layer.

Data Persistence layer stores the data in Amazon DynamoDB NoSQL database, Amazon RDS relational database and uploaded files are stored in Amazon S3.

Log Handling layer uses Amazon CloudTrail and Amazon CloudWatch Logs to ship the logs for processing to Datadog. Datadog provides a centralized logging service for Midaxo Cloud.

Network Security

As described in the shared responsibility model, the networking infrastructure for Midaxo Cloud is responsibility of AWS. Midaxo is responsible for configuring the access to different services utilizing AWS tools.

Midaxo Cloud is accessible via a browser, and all communication goes through AWS Web Application Firewall. All communication with client computers is encrypted with 256-bit SHA TLS certificates with 2048-bit key provisioned by Amazon Certificate Manager (ACM).

All AWS Services, including Web Application Firewall, are monitored 24/7 basis with Datadog security monitoring. For more information about monitoring, see the Monitoring and Logging section of this White Paper.

To ensure network security, the Midaxo office network that is used for administrative work is segregated from the Midaxo Cloud production environment.

Separate quality assurance and staging environments are used for testing. These environments are separated from the production environment.

Midaxo Cloud Security

The software architecture follows AWS' and Auth0's best practices for secure multi-tenant application design. Midaxo Cloud is developed by following secure software development practices, and a third-party security testing is performed for the new features.

Midaxo uses only well-known services or third-party libraries for product development and for delivering Midaxo Cloud. Midaxo maintains a list of all third-party components in use and regularly follows published vulnerabilities and software updates related to the third-party components.

Midaxo Cloud administrators use two-factor authentication and personal admin accounts when operating the Platform. Accounts are reviewed regularly, and passwords must meet length, complexity, and renewal requirements as defined in the Midaxo password policy.

Amazon Web Services platform security is proven by the following certifications and audits:

- SOC 1/ ISAE 3402
- SOC 2
- SOC 3
- Cloud Security Alliance (CSA) STAR registrant, and has completed the CSA Consensus Assessments Initiative Questionnaire (CAIQ)
- PCI DSS Level 1 compliance
- ISO 27001 Information Security Management – certification
- ISO 9001 Quality Management – certification

For more information about Amazon cloud platform security, visit the AWS Security Center.

Midaxo Cloud Application Security

Authentication

To access Midaxo Cloud, users are authenticated either with username and password, or with Single Sign-On using organizations identity provider. Supported SSO protocols are SAML 2.0 and Open ID Connect (OIDC).

Authenticated users get a security token to identify them. The token exchange uses the Authorization Flow with PKCE that secures the security token retrieval. In each request to the Midaxo Cloud API layer, the security token is checked. Based on the security token, a user can be authorized.

Midaxo Cloud uses Auth0 for authentication and authorization. Auth0 locks a user account after a defined number of failed login attempts. If a session is idle for 2 hours, it will expire automatically and require the user to log in again. Each session must reauthenticate again after 8 hours.

Midaxo Cloud enforces a strong password policy, which requires 12-character long passwords at minimum and passwords containing mixed case characters, including special characters.

Midaxo Cloud supports multi-factor authentication (MFA) with Time-based One-Time Password (TOTP) to strengthen the authentication process. Customer can also enforce MFA enrolment for all users in their Midaxo Cloud account.

Access Control

Customers are logically isolated in Midaxo Cloud. For a single customer, there can be multiple processes, deals, tasks, and documents, each separated using role-based access control.

Midaxo Cloud has requirements for end-user password length and complexity. Passwords are hashed and then stored in the Auth0 database. Hashing is implemented with the bcrypt algorithm and uses 10 salted rounds.

Each customer is granted one workspace admin account. The workspace admin is responsible for creating user accounts. Midaxo does not manage customer account credentials without a support request from the workspace admin.

Customer Data Security

Customers can choose to store their data exclusively in one of the Midaxo Cloud instances. Midaxo currently operates one instance in EU and one in US.

Customer data stored in the Midaxo EU instance is physically located in the AWS Ireland Region (Dublin). Customer data stored in Midaxo US instance is physically located in the AWS Ohio region. All data stored in every Midaxo Cloud instance is considered confidential.

Customers have ownership of their data. Midaxo's policy restricts Midaxo personnel, including admins, access to customer data to support purposes only when requested by the customer. The principle is that support is primarily conducted without accessing or seeing the customer's data and, secondarily, if necessary, by arranging a screen-sharing session or the customer granting temporary access rights to a project and data. Midaxo Cloud has technical controls in place to prevent Midaxo production administrators from accessing customer data and separate approval from Midaxo management is required for gaining access to customer data for production administrative tasks or for technical troubleshooting on support requests.

Customer account and all other customer data associated with the account are deleted automatically from Midaxo Cloud within 60 days of account termination or expiration. Data are still stored in daily backups, off-site backups, and snapshots for a year. After one year, the customer data are deleted completely in accordance with AWS' policy.

Data Security in Transit and at Rest

All end-to-end data transmissions are encrypted with 256-bit AES TLS. Transmissions between the client computer and the application use the HTTPS protocol with TLS 1.2 or newer protocol. Data stored in the Data Persistence layer is encrypted at rest and Amazon Key Management Service (KMS) is used for key management with 256-bit AES-GCM encryption keys. Keys are rotated annually.

Each customer's data are stored in databases that are logically isolated from other customers. Each row in the database is identified with customer's globally unique identifier as shown in the figure 4.

Guid	Customer Guid	…
3f9abd14-b94e-434a-a532-b22a161eb51c	7961f694-b0cb-4c51-97d9-0113b406ae0f	…
c99f5179-8dd7-4965-8a78-3eb56401c38c	7961f694-b0cb-4c51-97d9-0113b406ae0f	…
029d82fd-414f-43b8-93ba-4758b7574455	426fc032-9957-45da-a711-791cc4e11909	…

Figure 4 Customer Data Separation in Midaxo Cloud

Same isolation by customer's globally unique identifier is used within the document storage.

The use of access control list-based, item-level permissions provides a secondary safeguard against possible failures in data isolation between customer accounts. All stored deals, tasks, documents, etc. have item-level permissions, in addition to customer data isolation, to ensure that only authorized users can access them.

The possibility of circumventing access rights or isolation between customer accounts are analysed and tested in each development iteration by Midaxo's own development team, and periodically by an independent external auditor.

Malware detection

Midaxo Cloud scans all uploaded files for malware automatically and quarantines infected files, preventing all access to the file. Midaxo Cloud uses commercial grade anti-malware software for scanning.

Data breach notification practices

In case of a data breach or any other critical security incident, Midaxo always notifies the affected customers immediately upon discovery and informs them of the scope and mitigation activities. To date, Midaxo has never experienced any data breach incidents.

Data Release

Midaxo guarantees that customer data or log files are only released if demanded by a court order. Midaxo always notifies the customer prior to any release taking place.

Monitoring and Logging

Midaxo's monitoring team is always on standby for alarms generated by various automatic monitoring systems.

Midaxo Cloud's availability is monitored by an automated service with heartbeat functionality, ensuring that both front-end and back-end services are available and responding correctly. As Midaxo Cloud runs on AWS serverless technologies, AWS ensures the availability of computing resources.

The platform security is monitored in real time for threats and misconfigurations. Alarms generated by the SIEM solution are analyzed and escalated in a timely manner to Midaxo's incident management process to ensure proper incident response.

Login attempts to Midaxo Cloud are monitored to detect malicious attacks such as brute-force attacks on a customer's account. The number of allowed incorrect credential combinations is restricted, and abnormal activity is reported to the affected customer.

Midaxo Cloud application usage and access management events are logged, which allows Midaxo support to manually investigate potential cases of misuse reported by customers. Midaxo's access to the application log files is limited to named personnel, and Midaxo's policy only allows access for support purposes.

Furthermore, Midaxo Cloud system logs are monitored to detect any abnormal activity.

Midaxo Cloud Availability and Continuity

Backups and Redundancy

Midaxo Cloud data is automatically backed up daily. All backups are encrypted with Amazon KMS. The daily backups are stored for 90 days, and monthly backups are kept for one year.

All customer data can be fully recovered in case of hardware failure or an outage of the Amazon service. Midaxo Cloud runs on multiple Amazon availability zones and outages in a single availability zone do not affect the service availability.

Continuity and Disaster Recovery

Midaxo's business continuity plan covers various scenarios with prevention, response, and recovery strategies. The continuity plan is regularly updated based on a risk analysis, and Midaxo's monitoring team regularly tests the plans and work instructions.

Information about Midaxo Cloud outages will be published on the Midaxo website at https://support.midaxo.com and by email. Affected customers will be notified immediately upon discovery.

For details on Amazon Web service availability and disaster recovery, visit the following Web pages: http://aws.amazon.com/architecture/ and http://aws.amazon.com/backup-recovery/.

Physical Security

AWS Data Centers

AWS deploys comprehensive physical security measures to protect its data centers. To maintain certifications such as ISO/IEC 27001 Information Security Management, AWS is required to set up and maintain physical security controls such as video surveillance, physical access management, visitor access rules, and protection against exterior threats such as burglary or fire.

For more information about the physical security of AWS data centers, visit the AWS Security Center.

Midaxo Offices

Midaxo's offices are protected with the following physical security controls:

- Physical access: Physical access to Midaxo's offices is granted to authorized personnel only. Access rights are reviewed regularly.
- Badges: Midaxo personnel are required to wear badges at the Midaxo offices at all times. Badges are regularly renewed.
- Visitor access: Visitor access rules restrict visitor access to limited areas. All visitors are registered and escorted by Midaxo personnel.
- Protection against external threats: Midaxo's offices are protected with 24/7 video surveillance as well as intrusion and fire alarm systems.

Midaxo Cloud production data and customer data are not stored on Midaxo office premises.

Primary copies of software source code and other operation-critical data are stored off-site to ensure disaster recovery capabilities in crisis situations.

Midaxo's Information Security Management System

The information security management system has strategic importance to Midaxo, as Midaxo recognizes the importance of information security and confidentiality in the field of Corporate Development and M&A. Midaxo's information security management system is an integrated part of Midaxo's day-to-day operations and governance covering Midaxo's personnel, processes, and systems.

Policies for Information Security

Midaxo has internal information security policies defining Midaxo's security requirements and controls. Employee awareness is ensured through new employee induction and regular training thereafter. The policies are reviewed at least annually and approved by Midaxo's management team.

Roles and Responsibilities in Information Security

Midaxo's management team sets targets for information security and regularly reviews their current status. The management team acts as an information security steering group. Midaxo's CISO is responsible for information security management.

Processes

Midaxo has defined a set of processes to ensure information security in all its operations as well as in Midaxo Cloud.

Software Development, Testing, and Release

Midaxo utilizes Agile processes in software development, allowing the management of software releases from the development phase to release as an ongoing cycle of software development, testing, and release.

Midaxo has defined policies and procedures for software development, testing, and release management. Development and testing are performed in an environment that is separated from

the Midaxo Cloud production environment. Midaxo uses a Microsoft Visual Studio Code development environment and similar tooling, and Git for source code management.

Information security is integrated into the requirement definition, testing, and code review phases. In the requirement definition phase, information security is always considered based on a risk analysis. Vulnerabilities are tested during the software testing phase with test automation. Midaxo holds a code review meeting as part of development sprints. Midaxo uses peer review and automated tools for static code analysis. Additionally, Midaxo Cloud is continuously scanned for vulnerabilities using Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST) and Software Composition Analysis (SCA) tools. In addition to internal testing, Midaxo uses independent security expertise services companies regularly to perform penetration testing on the application.

Decision-making points are set to determine software versioning and the version to be released. Only a strictly limited number of development personnel have access to the software code repository or are authorized to make release decisions.

Vulnerability Management

Regarding vulnerability management, Midaxo maintains a list of all third-party components used in Midaxo Cloud and regularly follows published vulnerabilities and software updates related to the third-party components.

In addition, Midaxo closely monitors security updates, alerts, and advisories from various security organizations and authorities to monitor security threats and possible vulnerabilities. Based on risk analysis results, Midaxo deploys applicable mitigation methods and security controls when required.

Change Management

All changes to Midaxo Cloud and software are processed in accordance with the Midaxo change management process. The change management process ensures that all changes are properly planned, approved, and documented, and that associated risks are analyzed, and changes are implemented in a controlled manner.

Incident Management

Midaxo's customers can report incidents through the feedback function or by contacting customer support. Midaxo's policy holds each employee responsible for reporting perceived security incidents. Midaxo also receives alarms via various automatic channels. These are discussed in greater detail in the Monitoring and Logging section of this White Paper. Each alarm will be escalated as quickly as possible. Each incident will be analyzed to determine whether changes in the existing architecture or implementation are necessary. All reported incidents are logged, and the remedial action indicated. Critical security incidents and data breaches are always promptly reported to the affected customers upon discovery.

Access Control

Employee access to resources is limited to a role-based need to know basis. Access rights are granted, regularly reviewed, and deleted following the documented processes. Passwords must follow length, complexity, and renewal requirements as defined in Midaxo's password policy.

Access to the software code repository and the Midaxo Cloud production environment is restricted to a few software developer roles. The production environment requires two-factor authentication.

Other Processes

1. Risk management

   Internal and external risk analysis is performed regularly. Identified risks are managed with prevention, mitigation, response, and recovery strategies. Policies and processes are continuously improved based on the risk analysis findings.

2. Human resources

   Human resources ensure information security within processes for new personnel recruitment, during employment, and on termination of employment. For example, during recruitment, candidates are interviewed and background-checked, each new employee's induction includes Midaxo information security training, and information security awareness is maintained by regular training during employment.

3. Asset management

Midaxo manages an inventory of assets, and the acceptable use of assets is defined in the respective policies governing teleworking and mobile usage. Midaxo uses an information classification scheme to ensure that information is appropriately protected. Classified information is labeled and handled according to each classification. When assets, both electronic and paper, are no longer needed, disposal is handled securely according to formal procedures.

4. Supplier management

   Midaxo chooses suppliers carefully following a defined set of criteria. Supplier access to information is limited on a need to know basis, depending on the supplier's role and assigned responsibilities. Non-disclosure agreements are signed with suppliers.

5. Key management

   Midaxo's policy defines an information classification scheme and the acceptable use of classified information. The policy defines the use of cryptographic controls. For example, sensitive information is always transmitted in encrypted form. Cryptographic keys are stored in Amazon KMS securely outside the customer database instance.

Certifications & Audits

Midaxo has ISO/IEC 27001:2013 Information Security Management certification. ISO 27001 is an internationally recognized security management standard that specifies security management best practices and comprehensive security controls.

The Midaxo Cloud service is regularly penetration tested by independent information security expert services companies. Customers and prospects can download the latest attestations and/or certificates from Midaxo website when the companies provide such as part of their service or request information directly from Midaxo. The independent penetration testing verifies that the Midaxo Cloud architecture and software are designed, implemented, and maintained securely. Other independent third-party auditors and expert service companies regularly audit Midaxo Cloud's security.

In addition, customers have audited Midaxo Cloud. Midaxo offers customers the opportunity to perform security audits and penetration testing of their own with a test instance with the same architecture as in Midaxo Cloud.

Personal Data

Midaxo's practices for collecting, processing, protecting, and disclosing personal data are detailed in Midaxo's Privacy Policy.

The following personal data are processed and stored in Midaxo Cloud:

1. First and last name
2. Work email address
3. IP address

All customer data are stored in the AWS cloud service and are encrypted at-rest and in-motion. Main location of the data is AWS region in Dublin, Ireland for the Midaxo Cloud EU instance and AWS region in Ohio, United States for the Midaxo Cloud US instance.

For additional information on compliance provided by Amazon Web Services, see http://aws.amazon.com/compliance.

Disclaimer, Trademark and Copyright Notices

Disclaimer: This documentation is provided "as is" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are not enforceable by law. Midaxo shall not be held responsible, under any circumstances, for any indirect damage, including, but not limited to, any incidental or consequential loss (including monetary losses), that might result from the use of this documentation or the information disclosed in it. Information in this document is subject to change without prior notice.

Trademarks: The Midaxo name and the Midaxo logo are trademarks of Midaxo Ltd. Midaxo M&A Platform is a trademark of Midaxo Ltd. All third-party trademarks are the property of their respective owners.