INFORMATION SECURITY POLICY STATEMENT

Document ID	00118	Classification	External
Version Number	09	External	Douglas Gerhardt

Revision History

Version	Summary of Changes	Author	Date of Change
01	New document	Doug Gerhardt	17 March 2017
02	Formatting changes, and minor edits to match policies	Elizabeth Brand	28 February 2018
03	Modified Approvals	Doug Marzano	23 Jun. 19
04	Annual Review – Minot changes, updated policy numbers and titles	Martin Kukunovski	20 October 2020
05	Addition of IR policy, TOSM appendix and minor changes	Doug Gerhardt	01 April 2021
06	Renamed appendix to TOM to align terminologies	Doug Gerhardt	08 April 2021
07	Amendment to terminologies, minor corrections and additions	Doug Gerhardt	12 April 2021
08	Added statement in TOM around access specific to EDS	Doug Gerhardt	06 July 2021
09	Replacing data exporter with MarketAxess in Apx A g.(d)	Doug Gerhardt	03 December 2021

Review and Approvals

Title	Name	Version	Date
Chief Information Security Officer	Doug Marzano	09	December 3rd 2021 via MS Teams

Distribution

Name
For external Yes

Contents

Revision History 2
Review and Approvals 2
Distribution 2
1. Purpose 4
1. Policy Statement 4
2. Information Security Management System Objectives 4
3. Applicability 5
4. Specific Policies and Summary 6
5. Approval 7
6. Review 7
Appendix A – Technical and Organisational Measures 8

This policy applies to MarketAxess Holdings Inc. and its subsidiary entities ("MarketAxess", and together with its subsidiary entities, the "Group")

1. Purpose

This Information Security Policy Statement ("**Statement**") is intended to provide assurance in relation to some of the most commonly asked questions with respect to the information security procedures employed by The Group, but does not purport to be a comprehensive statement of the systems, controls, policies and procedures applicable to the Information Security Management System of The Group which includes, amongst other things, the policies and procedures listed in section 4 of this Statement and the Technical and Organisational Measures set out in Appendix A, to ensure the safeguarding of personal data pursuant to the General Data Protection Regulation (EU) 2016/679 ("**GDPR**")..

1. Policy Statement

The management body of The Group recognizes that the disciplines of confidentiality, integrity and availability in information security management are integral parts of its management function. The Group treats information security management as fundamental to achieving best business practice in relation to the adoption of appropriate information security controls, along the lines laid down in the ISO/IEC 27001:2013 standard.

The Group aims to meet the information security needs and expectations of its interested parties both within the organization, and from external parties including, amongst others, clients, suppliers, or relevant regulator, and considers the implementation of the security policies described herein as critical to The Group's integrity in maintaining its regulatory permissions and in its dealings with customers and suppliers.

The information security controls, policies and procedures of The Group (The Group "**Information Security Management System**") is designed to ensure that its systems are appropriately secured to achieve the Objectives.

2. Information Security Management System Objectives

The Group's Information Security Management System of The Group shall be designed to ensure, that The Group maintains physical, technical and organizational controls, to achieve at least the following objectives (the "**Objectives**"):

a) to prevent unauthorized use, disclosure, modification, damage or loss of Client data;

b) to protect Confidential Information and Client Data against unauthorised access;

c) to maintain confidentiality of Client Data and Confidential Information;

d) to avoid disclosure of Confidential Information and Client Data to unauthorised persons through deliberate or careless action;

e) to maintain integrity of Client Data through protection from unauthorised modification;

f) to restrict the availability of Confidential Information and Client Data to authorised users only when needed, maintaining the least privilege model;

g) to meet the requirements with respect to security as set out in Applicable Law and regulation, including;

- Article 9 of the Regulatory Technical Standard 13 pursuant to MiFIR for regulated Data Reporting Service Providers,
- the General Data Protection Regulation (EU) 2016/679, and
- the Sarbanes-Oxley Act of 2002;

h) to produce, maintain and test adequate business continuity and disaster recovery plans;

i) to provide appropriate security awareness training to all staff of The Group;

j) to report and investigate breaches of information security or suspected weaknesses in accordance with Applicable Law;

k) to identify, through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk and to manage the risks so identified.

l) to continually maintain and improve the ISMS as per ISO 27001:2013

m) to meet the Technical and Organisational Measures set out in Appendix A

3. Applicability

All staff and suppliers of The Group under a contract, who have any involvement with information or assets covered by the scope of the Information Security management system applicable to The Group Services, are responsible for implementing the principles embodied in the policies referred to in this Statement. All personnel have a responsibility for reporting security incidents and any identified weaknesses.

Any deliberate act to jeopardise the security of information that is the property of The Group or its customers will be subject to disciplinary and/or legal action as appropriate.

4. Specific Policies and Summary

The Group's Information Security Management System shall be supported by specific policies including but not limited to the policies described at a high level below:

- 00105 – **Security Awareness Training Policy**

  The Security Awareness policy is designed to ensures that staff of The Group understand the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as social engineering social engineering).

- 00108 – **Decommissioning and Data Destruction Policy**

  This Decommissioning and Data Destruction Policy establishes the secure disposal and destruction requirements necessary for MarketAxess to implement its strategic objectives for information governance in accordance with ISO27001:2013.

- 00110 – **Access Management Policy**

  The Account Management policy is designed to ensure that information system accounts are the only legitimate method by which The Group information systems may be accessed and to avoid access to The Group's information systems.

  The Account Management Policy applies to all information systems and information system components of The Group. Specifically, it includes applications that house transaction data, financial data, Client Data and personnel data. All information system accounts will be actively managed by appropriate administrative staff. Access to applications will only be granted with the approval of the noted business owner or delegate.

- 00112 – **Information Security Incident Management Policy**

  The purpose of this Information Security Incident Management Policy is to indicate the actions that must be taken in relation to identifying, assessing, discovering, managing monitoring and reporting Information Security Incidents.

  Where the Information Security Incident involves personal data (i.e., information relating to identifiable individuals, which we define broadly when making the analysis) some of the most significant obligations are MarketAxess' potential obligations under the EU GDPR.

- 00114 – **Physical Security Policy**

  The Physical Security Policy details the required controls, procedures and scope required to protect the environments where The Group's and/or its clients' confidential data in including

Client Data is processed and stored. The document has been produced in line with the requirements and guidance contained in ISO27001:2013.

- 00119 – **Firewall Policy**

  This policy provides for firewalls to be operated between networks to create a secure operating environment for The Group computer and network resources. The purpose of this policy is to dictate how firewalls should handle network traffic for specific zones.

- 00126 – **Backup and Restoration Policy**

  The Backup Policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

5. Approval

The management body of The Group is responsible for oversight of the Information Security Management System.

The Group Chief Information Security Officer facilitates the implementation of the policies referred to herein through the appropriate standards and procedures.

The Head of Information Security EMEA & APAC is responsible for keeping the management body of the Group informed of the requirements of and to ensure compliance with the locally applicable regulations.

This Statement is subject to the approval of the Chief Information Security Officer of The Group.

6. Review

This policy is reviewed regularly and, in case of influencing changed, to ensure it remains appropriate for the business and our ability to serve our customers.

Appendix A – Technical and Organisational Measures

In this Appendix the term "personal data" has the meaning given in the GDPR and the measures set out below are, amongst other things, designed to meet the requirements of the GDPR with respect to the safeguarding of personal data. The measures set out in this Appendix apply equally to all privacy related data regardless of the jurisdiction of the data subject, and all sensitive data generally.

a. Organization of Information Security

(a) **Security Ownership.** MarketAxess has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

(b) **Security Roles and Responsibilities.** MarketAxess personnel with access to personal data are subject to confidentiality obligations.

(c) **Risk Management.** MarketAxess has performed a risk assessment before processing personal data or offering the Services in scope of the ISMS and perform Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals.

b. Human Resources Security

(a) **General**. MarketAxess informs its personnel about relevant security procedures and their respective roles. MarketAxess also informs its personnel of possible consequences of breaching its security policies and procedures. Employees who violate MarketAxess security policies may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of his or her contract or assignment with MarketAxess.

(b) **Training.** MarketAxess personnel with access to personal data receive:

i. annual security education and training regarding privacy and security procedures for the Services to aid in the prevention of unauthorized use (or inadvertent disclosure) of personal data;

ii. training regarding effectively responding to security events; and

iii. training is regularly reinforced through refresher training courses, emails, posters, notice boards and other training materials.

(c) **Background Checks.** Subject to Applicable Law, MarketAxess personnel are subject to criminal background checks.

c. Asset Management

(a) **Asset Inventory.** Assets associated with information and information-processing facilities are identified and an inventory of assets is maintained.

(b) **Information Classification.** MarketAxess classifies data, including personal data, to help identify it and to allow for access to it to be appropriately restricted.

(c) **Media Handling**

MarketAxess personnel:

i. use trusted devices that are configured with security software and automatic patching;

ii. follow MarketAxess' hardening standards when accessing personal data or when having personal data in his/her control;

iii. avoid accepting or storing personal data on a non-trusted device (meaning one that does not comply to MarketAxess' hardening standard). This includes smartphones, tablets, USB drives and CDs that do not meet MarketAxess' hardening standards;

iv. encrypt personal data stored on a mobile device, including laptops, smartphones, tables, USB drives and CDs; and

v. take measures to prevent accidental exposure of personal data, including using privacy filters on laptops when in areas where over-the-shoulder viewing of personal data is possible.

d. Personnel Access Controls

(a) **Access Policy.** An access control policy is established, documented, and reviewed based on business and information security requirements.

(b) **Access Recordkeeping.** MarketAxess maintains a record of security privileges of its personnel that have access to personal data, networks and network services.

(c) **Access Authorization**

i. MarketAxess has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to MarketAxess' systems and networks at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. MarketAxess maintains and updates a record of personnel authorized to access systems that contain personal data.

iii. for systems that process personal data, MarketAxess revalidates access of users who change reporting structure and deactivates authentication credentials that have not been used for a period not to exceed six months.

iv. MarketAxess identifies those personnel who may grant, alter or cancel authorized access to data, systems and networks.

v. MarketAxess ensures that, each personnel having access to its systems have a single unique identifier/log-in.

vi. MarketAxess maintains strict policies against any shared "generic" user identification access.

(d) For customer personal data stored in EDS systems, MarketAxess has a strict policy that denies any access (including view only access) to personal data in the clear by any employee regardless of their geographical location. A controlled access procedure, which requires at a minimum the approval of an EU based director of MAPT BV; and UK senior executive approval, is clearly defined, in case of support emergencies only (for a limited time period in each case as necessary). In such case access will ONLY be granted to employees based in the EU/UK.**Network Design.** For systems that process personal data, MarketAxess has controls to avoid personnel assuming access rights they have not been assigned to gain unauthorized access to personal data.

(e) **Least Privilege.** MarketAxess limits access to personal data to those MarketAxess personnel performing the Services and, to the extent technical support is needed, its personnel performing such technical support.

(f) **Integrity and Confidentiality**

i. MarketAxess instructs its personnel to automatically lock screens and/or disable administrative sessions when leaving premises that are controlled by MarketAxess or when computers are otherwise left unattended.

ii. MarketAxess computers and trusted devices automatically lock after ten (10) minutes of inactivity.

iii. MarketAxess stores passwords in a secured and restricted way that makes them unintelligible while they are in force.

(g) **Authentication**

i. MarketAxess uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, MarketAxess requires that the passwords be renewed regularly, no less often than every 3 months.

ii. Where authentication mechanisms are based on passwords, MarketAxess requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

iii. MarketAxess ensures that de-activated or expired identifiers are not granted to other individuals.

iv. MarketAxess monitors repeated attempts to gain access to the information system using an invalid password.

v. MarketAxess maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vi. MarketAxess limits access to file stores and/or systems in which passwords are stored.

e. Cryptography

(a) **Cryptographic controls policy**

i. MarketAxess has a policy on the use of cryptographic controls based on assessed risks and data classification levels.

ii. MarketAxess assesses and manages the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths, according to NIST standards.

iii. MarketAxess' cryptographic controls/policy addresses appropriate algorithm selections, key management, and other core features of cryptographic implementations, in line with ISO27001 and NIST SP 800-57.

(b) **Key management.** MarketAxess has procedures for securely distributing, storing, archiving and changing/updating keys; recovering, revoking/destroying and dealing with compromised keys; and logging all transactions associated with keys.

f. Physical and Environmental Security

(a) **Physical Access to Facilities**

i. MarketAxess limits access to facilities where systems that process personal data are located to authorized individuals.

ii. access is controlled through key card and/or appropriate sign-in procedures for facilities with systems processing personal data. Personnel must be registered and are required to carry appropriate identification badges.

(b) **Physical Access to Equipment.** MarketAxess equipment that is located off premises is protected using industry standard process to limit access to authorized individuals.

(c) **Protection from Disruptions.** MarketAxess uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

(d) **Clear Desk.** MarketAxess has policies requiring a "clean desk/clear screen" at the end of the workday.

g. Operations Security

(a) **Operational Policy.** MarketAxess maintains policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to personal data and to its systems and networks.

(b) **Workstations.** MarketAxess uses the following controls on its workstations that process personal data:

i. anti-malware software and firewalls;

ii. password and screensaver controls with automatic lock of workstation upon idleness;

iii. periodic scans to query the hardware and the presence of software, patches, corporate applications, and security components; and

iv. full disk encryption on laptop devices.

(c) **Mobile Devices.** Mobile phones and tablets are protected via a mandatory PIN, restrictions on amount of email that can be stored on the device, and a remote wipe capability.

(d) **Data Recovery.** MarketAxess maintains multiple copies of personal data from which personal data can be recovered. MarketAxess stores copies of personal data and data recovery procedures in a different place from where the primary equipment processing the personal data is located. MarketAxess has specific procedures in place governing access to these copies of personal data.

(e) **Logging and Monitoring.** MarketAxess maintains logs of and monitors access to administrator and operator activity and data recovery events.

h. Communications Security and Data Transfer

(a) **Networks.** MarketAxess uses the following controls to secure its networks which store personal data:

i. network traffic passes through firewalls, which are monitored. MarketAxess has implemented intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected 24x7;

ii. anti-spoofing filters are enabled on routers;

iii. network, application and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days;

iv. initial user passwords are required to be changed during the first logon. MarketAxess policy prohibits the sharing of user IDs and passwords; and

v. firewalls are deployed to protect the perimeter data exporter network.

(b) **Virtual Private Networks ("VPN").** When remote connectivity to the data exporter network is required for processing of personal data, MarketAxess uses VPN servers for the remote access with the following or similar capabilities:

i. supports strong encryption such as AES-256 and RSA2048;

ii. connections from customers to MarketAxess locations are only established using secure channels approved by both parties;

iii. the use of two-factor authentication is required.

i. System Acquisition, Development and Maintenance

(a) **Security Requirements.** MarketAxess has adopted security requirements for the purchase or development of information systems, including for application services delivered through public networks.

(b) **Development Requirements.** MarketAxess has policies for secure development, system engineering and support. Processor conducts appropriate tests for system security as part of acceptance testing processes.

j. Supplier Relationships

(a) **Policies.** MarketAxess has information security policies or procedures for its use of suppliers. MarketAxess has agreements with suppliers in which they agree to comply with MarketAxess' security requirements.

(b) **Management.** MarketAxess performs periodic audits on key suppliers and manages service delivery by its suppliers and reviews security against the agreements with suppliers.

k. Information Security Incident Management

(a) **Response Process.** MarketAxess maintains a record of information security breaches with a description of the breach, the consequences of the breach, the name of the reporter and to whom the breach was reported, and the procedure for recovering data.

(b) **Reporting.** MarketAxess will report without undue delay, and in any event within 48 hours, to data exporter any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

l. Information Security Aspects of Business Continuity Management

(a) **Planning.** MarketAxess maintains emergency and contingency plans for the facilities in which MarketAxess information systems that process personal data are located.

(b) **Data Recovery.** MarketAxess' redundant storage and its procedures for recovering data are designed to attempt to reconstruct personal data in its original state from before the time it was lost or destroyed.