Closed Circuit Television (CCTV) Policy

V1. – July 2024

Review and Approval	
Version	1
Approved by	Board of Directors
Date Last Reviewed	July 2024
Review Frequency	Annual
Next Review Date	December 2024
Policy Owner	Petros Petrou, Head of Technology

Version Recording		
Date	**Version**	**Changes made**
July 2024	1	• Basic Document outline • Policy formed in line with the Data Protection Health Check Report

Contents

1. **Introduction:**

1.1 1.1 M4Markets is a brand name of Harindale Ltd (hereinafter called as the "**Company**" or "**M4Markets**" or "**we**" or "**our**" or "**us**"). The Company is a private limited liability company by shares, incorporated and existing under the laws of the Republic of Cyprus, with registration number HE 346662. The Company is authorized and licensed by the Cyprus Securities and Exchange Commission (hereafter the "**CySEC**") to operate as an Investment Firm, under the license number 301/16.

1.2 Closed-Circuit Television (CCTV) systems have become integral to modern security infrastructure, offering a robust mechanism for monitoring and safeguarding various environments. Implementing a comprehensive CCTV policy is essential to ensure that these surveillance systems are utilized effectively and responsibly. Such a policy outlines the objectives of surveillance, delineates the roles and responsibilities of personnel, and establishes clear guidelines for installing, operating, and maintaining CCTV equipment. Additionally, it addresses critical issues such as privacy concerns, data protection, and compliance with legal and regulatory requirements. By providing a structured framework, a well-crafted CCTV policy not only enhances security and safety but also fosters transparency and trust among stakeholders.

2. **Purpose:**

2.1 By virtue of Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), which applies as of 25 May 2018 (hereinafter the "GDPR") and Law 125(I)/2018 of the Republic of Cyprus (hereinafter the "Data Protection Law"), as these are amended from time to time, individuals have the right to be informed about the collection and use of their Personal Data in a concise, transparent, intelligible and easily accessible from using clear and plain language. Where Personal Data relating to a Data Subject is collected either directly from the Data Subject or from a third party, the Controller must provide the Data Subject with specific information, as such is set out in Articles 13 and 14 of the GDPR. Where the Personal Data is collected directly from the Data Subject, the information must be provided to the Data Subject at

the time the Personal Data is obtained. Any new uses of a Data Subject's personal data must be brought to the attention of the Data Subject before such new Processing takes place.

2.2 This Closed-Circuit Television (CCTV) Policy (hereinafter the "Policy") describes the video-surveillance system established and maintained by the Company in the Premises (the "CCTV System"), and the measures taken by the Company to protect personal data, privacy and the other fundamental rights, as a Controller, under the GDPR and the Data Protection Law.

2.3 Terms such as Personal Data, Data Subject, Processing, Controller and Processor which are used in this Policy have the meaning set out to them in the GDPR.

3. Scope

3.1 This Policy describes the type of Personal Data the Company, and the companies within the group of companies of the Company having their offices in the same premises with the Company, collects from its visitors and employees when visiting the Company's premises (hereinafter the "Premises") and how the Company Processes this Personal Data.

4. Privacy, data protection, and the conformity of the CCTV System

4.1 The CCTV System

The CCTV System and the Company's procedures are in line with GDPR and the Data Protection Law.

4.2 Compliance status

The Company collects and processes the images in compliance with the GDPR and the Data Protection Law.

4.3 Internal audit

An internal audit shall be carried out every year.

4.4 Transparency

This Policy is available on the Premises and the Company's website at https://www.m4markets.eu/about/legal-documents.

4.5 Periodic checks

Every year, the Company carries out a check concerning data protection.

At the time of those periodic checks, an analysis is made of:

i. the suitability of the CCTV system in place to meet the objectives laid down;

ii. the need for amendments and/or adjustments to the CCTV System; or

iii. the lack of adequate alternatives.

The periodic checks are intended to ascertain whether this Policy and the CCTV System in place remain in line with the GDPR, the Data Protection Law, and relevant guidelines and decisions (suitability audit) and whether the Policy is applied in practice (compliance audit).

4.6 Technical solutions favoring privacy

The Company has implemented the following technological solutions concerning privacy:

i. The viewpoints and the cameras have been placed in such a way as to cover only the areas to be monitored.

ii. The areas of the buildings where the expectation of privacy is even higher are not monitored by cameras.

iii. Specific software, a user profile, and a password are required for the personnel authorised, a small number of members of the relevant department of the Company, to access the images recorded; and

iv. All activity on the system is recorded (recording of the activity and the relevant active user).

5. **Locations under surveillance**

5.1 According to the needs of the Company, a CCTV System of 5 cameras has been installed and is maintained on the premises.

5.2 The CCTV System covers (hereinafter the "Surveillance Areas"):

I. External surfaces/Emergency exits.

Objective: to deter any attempt to gain access and to deter offensive actions.

II. Access to the various buildings' reception and reception desk.

Objective: to monitor the flow of entries and exits.

III. Access to the car park (barriers and gates)/Ramps and traffic routes in the car park.

Objective: to deter any damage to the Company's assets or assaults on persons and to assist in the resolution of disputes in that regard.

IV. Equipment.

Objective: to monitor the equipment and protect sensitive technical installations.

V. Public areas inside the buildings.

Objective: to enable the Company to have an overview of the general situation so that it may react to any incident (disorderly conduct, a suspect abandoned package, a person suffering a fall, etc.); surveillance of the works of art; rapid intervention in the event of fire or illness.

VI. Passages to private protected areas.

Objective: to prevent any attempt to gain unlawful access to those areas and assist users with difficulties connected with the access control equipment (access gates or badge readers).

5.3 Plans showing the placement of the cameras are available at the Security and Safety Department or the IT Department of the Company and may be consulted there. Those plans are also available, on request by email, to the Data Protection Officer of the Company (hereinafter the "DPO") at dpo@m4markets.eu.

5.4 No cameras cover locations where people may expect greater respect for their privacy.

6. Personal Data collected and the reason for their collection

6.1 Brief description and detailed technical specifications of the CCTV System

The CCTV System records digital images and is equipped with a movement detection system. The CCTV System records movements detected by the cameras in the Surveillance Areas and the date, time, and location. The cameras function 24 hours a day, 7 days a week. The image quality, depending on the settings, can enable people to be identified. All the cameras are fixed. The CCTV System does not use so-called intelligent technologies, is not connected to other systems, does not use covert surveillance, does not record sound signals, and does not use 'speech-enabled surveillance cameras.

6.2 The objective of the surveillance

The Company uses its CCTV System exclusively to monitor access and security (the security of persons, buildings, and information). Those installations supplement the access control systems, the emergency exit management systems, and the fire safety systems. The CCTV System forms part of the group of measures put in place to strengthen the general security policy and helps to prevent, deter and, if necessary, investigate any unlawful access (high-risk locations, IT infrastructures, and operational information). In addition, video surveillance helps to prevent, detect, and investigate thefts of equipment or property belonging to the Company, its employees, or visitors. The CCTV System also contributes to ensuring the safety of the users of the Premises (for example, in the event of fire, assault, etc.).

6.3 Limitation of scope

Video surveillance is used solely for the purposes set out above. The CCTV System is not used to assess the work of employees or to check their presence. The CCTV System is used as an aid to investigation only in the event of a security incident (thefts, unauthorised access, etc.) and, exceptionally, images may be transferred to any third parties in the exercise of their powers and duties. Those transfers are described in Chapter 8.5 "Transfers and Disclosure" below.

6.4 Webcams

There are no webcams connected to the CCTV System of the Company.

6.5 Collection of special categories of data

No data in the special categories of data referred to in the GDPR and the Data Protection Law (i.e., inter alia, political opinions. religious or philosophical beliefs. trade-union membership. genetic, biometric, or health data except in specific cases) is collected. If demonstrations were to be held outside the premises, the following additional guarantees are in place:

i. Demonstrations are monitored only for security reasons.

ii. The cameras cannot be fixed on faces and must not attempt to identify appearances, save in the event of an imminent threat to public safety or violent criminal behaviour (vandalism, attacks).

iii. The images cannot be used for data-mining purposes; and

iv. All those who operate the video installations shall receive training (see point "Data Protection Training" below) to avoid any disproportionate effect on the privacy and other fundamental rights of the participants filmed, including their freedom of assembly.

7. Legitimacy and Legal Basis of the CCTV System

7.1 Use of the CCTV System for security and access control purposes is necessary to ensure the smooth running of the Company and the legitimate exercise of the authority vested in it. The use of the CCTV System, as it is operated by the Company, complies with the GDPR and the Data Protection Law. This Policy, which forms part of a wider series of security policies adopted by the Company, provides a more detailed and specific legal basis for video surveillance.

8. Access to Information and Data Collected

8.1 Security and Safety Department of the Company

The members of the Technology Department of the Company (hereinafter the "Technology Department") have access to the real-time images transmitted in cases of emergency. It is not possible for anyone else to access the recorded images. The specifications annexed to the services contract concluded with the Technology Department contain confidentiality and data protection clauses to ensure that the Technology Department upholds the protection of Personal Data. The recorded images are accessible only to the staff of the Technology Department. All members of the Technology Department are required to sign a statement of confidentiality concerning the use of the CCTV System.

8.2 Access rights

Specific software, a user profile, and a password are necessary to have access to the images recorded. That specific software is installed on the computers of only certain members of the Technology Department. The Technology Department is acting then as a processor for the GDPR and the Data Protection Law.

8.3 Data protection training

All staff having access to the CCTV System have received training on data protection.

8.4 The security staff's confidentiality undertaking

Each member of the Technology Department, who has the right to Process images has signed a confidentiality undertaking after undergoing data protection training.

8.5 Transfers and disclosure

No transfer or disclosure of Personal Data shall be made except by the Head of the Technology Department, after consulting the DPO. Any transfer or disclosure of Personal Data to addresses external to the Technology Department shall be subject to a thorough assessment as regards the need and compatibility of its purpose with the purpose initially pursued, namely security and access control. Such transfers shall be systematically recorded in the "retention and transfer register" held by the Head of the Technology Department.

8.5.1 Requests for disclosure:

i. The Company may share data with its insurance company and/or its lawyers and/or the competent police, where the Company considers that this is reasonably necessary for any of the legitimate purposes of the Company.

ii. No images from the CCTV System will be disclosed to any other third party, without express permission being given by the DPO. Personal Data will not normally be released unless satisfactory evidence that is required for legal proceedings or under a court order has been produced.

iii. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

iv. We will maintain a record of all disclosures of CCTV footage; and

v. No images from the CCTV System will ever be posted online or disclosed to the media.

9. **Data and Information protection measures**

9.1 The principal technical and organisational measures put into place to protect the security of the CCTV system, including Personal Data, are as follows:

i. The servers on which the images are recorded are sited in secure locations, protected by physical security measures; firewalls are installed to protect the IT installations.

ii. Each member of the Security and Safety Department, and each of the security guards from the Security Firm, has signed a confidentiality undertaking.

iii. User access rights to the CCTV system are restricted to the tools necessary to carry out their work; and

iv. Only the system manager, designated by the Company, is authorised to grant, modify or cancel user access rights. The grant, modification, or cancellation of access rights is carried out in accordance with the criteria laid down in the Internal video surveillance procedure.

10. **Retention of Data**

10.1 The images/recordings are retained for a maximum of 60 days. After 60 days, the images/recordings are automatically erased.

10.2 That period is justified by:

i. Current experience is that security incidents are often reported to the Technology Department more than 2-3 weeks after they occur.

ii. The practice of criminals/terrorists inspecting the buildings before committing an unlawful act.

iii. The high number of visitors per year. Certain images may be retained longer if that retention is necessary for an inquiry or to serve as evidence related to a security incident. That retention is documented

(electronic register) and the reasons for retaining the images for more than 60 days are stated. The need for that retention shall be regularly re-assessed.

11. **Public information and specific individual information**

11.1 Information via various media

Appropriate and full information on the CCTV System should be made available to the public. That information shall be provided via the following media:

i. Warning signs are placed at the various building access points and public places and advise of the presence of a CCTV System.

ii. This policy is available on the Premises and on the Company's website at https://www.m4markets.eu/about/legal-documents.

11.2 Specific individual notification

When persons are identified on the images (for example, for a security investigation), they must be informed of that fact individually if at least one of the following conditions is satisfied:

- Their identity is noted in a file.

- The video sequence is used against the person in question.

- The video sequence is retained for a period longer than the period prescribed.

- The video sequence is transferred outside the Security and Safety Section.

- The identity of the person is communicated to people outside the company premises. Provision of that individual information may be delayed, by the Data Protection Law and the GDPR, if that is necessary to ensure the prevention, investigation, detection, or prosecution of criminal offences. The DPO shall be consulted if the application of this restriction is envisaged.

12. Rights of the Data Subjects

12.1 For clients of the Company: Please refer to the privacy policy of the Company available at https://www.m4markets.eu/about/legal-documents.

All requests for access, rectification, restriction, objection, erasure or data portability or questions must be addressed to the DPO of the Company by post at the postal address: Spyrou Kyprianou Avenue 78, MAGNUM BUSINESS CENTER, 2nd Floor, P.C. 3076, Limassol, Cyprus or by sending an email at: dpo@m4markets.eu.

12.2 The Security and Safety Department or the DPO can also be contacted for any other questions concerning the processing of personal data as regards the CCTV System put into place in the Court.

12.3 If you have any grounds to believe that the Company does not appropriately use your data, you can further submit a complaint to the commissioner for personal data protection of the Republic of Cyprus. Further details are available at the Website link: http://www.dataprotection.gov.cy.

13. Changes to the Policy

13.1 The Company reserves the right to change or amend this Policy without further notice to you, provided that the changes do not significantly reduce your rights under this Policy. If the Company makes material changes to this Policy, the Company will notify you by email or utilizing a notice on the Company's home page or by changing the version of the document uploaded on the Company's website, including the date of the update which will be visible to the first page of this document. In the latter case, any such amended Policy will be effective immediately once it is uploaded on the Company's website.

13.2 The latest and prevailing version of this Policy will always be available at https://www.m4markets.eu/about/legal-documents. Similarly, a copy of the Policy will be readily available to the public at the reception of the Company's premises and will be provided to the public upon request.

E: support@m4markets.eu