


Data Protection Policy
March 2026
V 2.1

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

1. Introduction

The General Data Protection Regulation (GDPR) aims at harmonising data protection laws in the EU that are fit for purpose in the digital age. The way data is collected, stored and used has changed fundamentally in the past 25 years and with the growth of the internet and the amount of data held growing exponentially, the existing data protection rules can no longer be deemed sufficient.

By introducing a single law, the EU believes that it will bring better transparency to help support the rights of individuals and grow the digital economy. GDPR imposes rules on companies, government agencies and other organisations that offer goods and services to people within the EU, or those that collect and analyse data tied to EU residents. From an economic standpoint, the GDPR aims to simplify the regulatory environment for international business by unifying the regulation within the EU.

The primary objective of the GDPR is 'To harmonise Data Privacy Laws across Europe' and is about individuals rights over information about themselves; when it may be obtained, how it must be protected, and what may or may not be done with it.

2. Legal Framework

The current legislation for the processing and protection of personal data in Cyprus is the Processing of Personal Data (Protection of the Individual) Law of 2001 (the "Law").

The Law is based on the European Directive 95/46/EC of the European Parliament and of the Council of the 24th of October 1995 (the "Directive") and has a twofold purpose; the protection of the fundamental rights and privacy of individuals and ensure the free circulation of personal data in the

Member States in order to achieve economic and social progress; and the technical and scientific cooperation in the ever-increasing information and telecommunication society.

The implementing legislation for the General Data Protection Regulations ("GDPR") is, Regulation

- (EU) 2016/679 of the European Parliament and the Council of 27th April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. GDPR replaces and repeals directive 95/46/EC.

In Cyprus, the Office of the Commissioner for Personal Data Protection is responsible for implementing existing legislation in relation to data protection. Cyprus is currently drafting a bill for

GDPR implementation which will replace Law 138(I)/2001.

Because the GDPR is a regulation and not a directive, it means that it is directly applicable in all EU member states from May 2018. A directive only directs member states to implement ruling but does not enforce.

3. The Company

UBK Markets Ltd is authorised and regulated by the Cyprus Securities and Exchange Commission (CySEC), license number 186/12 and registered at 67, Spyrou Kyprianou Avenue, Kyriakides Business Center, 2nd Floor, CY-4003 Limassol, Cyprus.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

UBK Markets LTD (hereinafter, “The Company”) is committed to protecting the rights and privacy of individuals in accordance with relevant legislation such as applicable Data Protection Acts, in any jurisdiction in which it does business.

The Company has overall responsibility for ensuring compliance with applicable Data Protection legislation. All Employees who collect or control the contents and use of personal data are also responsible for compliance with the applicable legislation. The Company will provide support and training to all Employees to ensure they are in a position to comply with the legislation.

4. Data Protection – An Overview

Date Protection Principals (Article 5):

Data must be:

- ☒ Processed lawfully, fairly and in a transparent manner
- ☒ Collected for specific, explicit and legitimate purposes (purpose limitation)
- ☒ Adequate, relevant and limited to what is necessary for the purposes (data minimisation)
- ☒ Accurate and kept up to date – erroneous data erased or rectified without delay (accuracy)
- ☒ Kept for no longer than is necessary for the purposes (storage limitation)
- ☒ Stored with appropriate security, protection against unauthorised or unlawful processing, no accidental loss, destruction or damage (integrity and confidentiality)

Who does the GDPR apply to?

The GDPR applies to processing of personal data carried out by organisations operating within the EU as well as organisations outside the EU that offer goods or services to individuals in the EU. GDPR categorises organisations as either ‘Controllers’ and/or ‘Processors’. Controllers determine the purposes and means of processing personal data, whereas Processors are responsible for processing personal data on behalf on a Controller.

Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

For the purposes of GDPR, UBK Markets are considered to be both Controllers and Processors.

Depending on the category of data subject UBK Markets may utilise third parties in other jurisdictions to act as Processors.


What information does the GDPR apply to?

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier

The GDPR refers to sensitive personal data as “special categories of personal data”

5. Data Protection Officer

The GDPR requires certain companies to have a designated Data Protection Officer (DPO) whose duties and responsibilities are listed below.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

The Company has appointed a DPO who has the requisite expertise commensurate with the complexity and sensitivity of the data being processed and who holds a complete understanding of

GDPR. The DPO reports directly to the Board of Directors and has no conflict of interest.

The duties of the DPO include:

- ☒ Ensuring compliance with the GDPR, local laws and legislation;
- ☒ Provision of training and ensuring that employees are aware of their obligations per the

GDPR;

- ☒ Completion of DPIA's; and,
- ☒ Cooperate and act as a point of contact on GDPR matters on behalf of The Company.
- ☒ Review all policies, procedures and controls to ensure that data is
- ☒ processed lawfully, fairly and transparently,
- ☒ collected for specific, explicit and legitimate purposes,
- ☒ is limited to what is necessary for the Data Subject,
- ☒ is accurate and where identified by the Data Subject or by The Company that data is not accurate, take appropriate action to rectify or correct
- ☒ is held for a minimum period, depending on various legislation, after the relationship with the data subject has terminated

6. Lawful basis for processing

According to GDPR, all Companies must have a valid lawful basis in order to process personal data.


There are six available lawful bases for processing. No single basis is considered 'better' or more important than the others, however the basis used will depend on your purpose and relationship with the individual (Data Subject).

Most lawful bases require that processing is 'necessary' and if a Company can reasonably achieve the same purpose without the processing, then there is no lawful basis. Lawful basis should be determined before processing begins and should be documented in both The Company's internal records and privacy notices, along with the purpose for processing.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

- a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

- c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- d) Vital interests: the processing is necessary to protect someone's life.
- e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The highlighted lawful bases are those which apply to various processing of personal data by the Company. For more information on specific lawful basis and purpose of processing related to individual processes, please refer to The Company's Information Asset Register (IAR).

It should be noted that the Company may utilise more than one lawful basis for the collection of data in relation to its data subjects.

6.1 Consent

The Company does not rely solely on Consent as a means of lawful basis for any processing of personal data, although data is collected from data subjects with their consent either through various agreements and/or through the actual collection of the data directly from the data subject themselves.

According to GDPR, Consent means offering data subjects real choice and control, all data subjects have control over the data they provide to the Company and are fully aware of the purposes for the data collection.

The Company keeps a record of when and how consent is collected from the data subject in its IAR ensuring to regularly review and refresh consents at appropriate intervals when and if this is deemed necessary.

Practical application will usually apply to:

☒ Application forms for Client/Introducing Broker Accounts; and, ☒ Employer/employee relationship ☒ Third Party service providers


6.2 Contract

The Company has in place, with various data subjects, contracts and agreements and uses this lawful basis to process data subject's personal data to fulfil contractual obligations. The processing of the data under this lawful basis must always be necessary, thereby if the Company could reasonably do what is needed without the processing of personal data, this basis will not apply.

The decision to rely on this lawful basis and justification is documented in the Company's IAR.

Practical application will usually apply to:

☒ Client Agreements

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

- ☒ Introducing Broker Agreements
- ☒ Employment Agreements
- ☒ Third Party/Vendor Agreements

6.3 Legal obligation

As a licensed Cypriot Investment Firm (CIF), the Company is subject to various laws and regulations issued by the Cyprus Securities and Exchange Commission (CySEC) in order to maintain its license and authorisation. In addition, various legislation related to companies incorporated in Cyprus may apply, such as the obligation to pay tax and social insurance on behalf of employees.

Reliance on this lawful basis is made when the process of personal data is needed to comply with common law of statutory obligation.

The decision to rely on this lawful basis, the justification, as well as the specific legal provision is set out in the Company's IAR. Legal obligation generally includes:

- ☒ Customer Identification and Due Diligence in accordance with articles 60-66 of The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007-2019 and Amending Laws 158(I)/2018 and 81(I)/2019 and Part V of The Cyprus Securities and Exchange Commission Directive for the prevention and suppression of money laundering and terrorist financing of 2019 or any subsequent amendments ☒ L.87(I)/2017 Law for the provision of investments services, the exercise of investment activities and the operation of regulated markets ☒ Regulation 596/2014; Regulation (EU) No 648/2012; Regulation (EU) No 600/2014 ☒ Assessment and Collection of Taxes Laws of 1978 - 2015 ☒ CRS Decree: Assessment and Collection of Taxes (Exchange of Information) in the frame of the Multilateral Competent Authority Agreement ☒ Automatic Exchange of Financial Account Information Decree of 2016

6.4 Legitimate Interest

Legitimate Interest is different to the other lawful bases as it is not centred around a particular purpose (e.g. performing a contract with the individual or complying with a legal obligation) and could in principle apply to any type of processing for any reasonable purpose.

When determining whether legitimate interest can be used as a lawful basis for the collection of data, the Company may apply the following three-part test:

1. Purpose Test: Is there a legitimate interest behind the processing of the data?
2. Necessity Test: Is the processing necessary for that purpose?
3. Balancing Test: Is the legitimate interest overridden by the data subject's interests, rights or freedoms?

The processing of personal data under this lawful basis is considered by the Company to fall into one of the following categories:

- ☒ Internal administrative purposes relating to the data subject ☒ Marketing ☒ Developing new products and services and improving existing products (e.g. correcting errors, developing greater ease of use for more actively used services)

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

☒ Processing personal data to prevent fraud

☒ Security risk management and resolve disputes in court or extra judicially ☒ Legal compliance requirements ☒ To report Money Laundering and Terrorist Financing to a competent authority ☒ Internal corporate governance

In all instances the legitimate interest is documented in the Company's IAR.

6.5 Criminal offence data

To process personal data about criminal convictions or offenses, the Company is required to have both a lawful basis, under Article 6 and either legal authority or official authority for the processing under Article 10.

The Company for the purposes of fulfilling its legal obligation to apply Enhanced Due Diligence (EDD) of high-risk clients, utilises a risk intelligence data screening system called World- Check. The source of risk intelligence helps the Company to meet its regulatory obligations, make informed decisions and help prevent the Company from inadvertently being used to launder the proceeds of crime or association with corrupt business practices.

The Company uses the full name of the data subject to screen against data that is derived from sources available to the general public, including:

☒ 600+ sanction, watch, regulatory and law enforcement lists ☒ Local and international government records ☒ Country specific data sources ☒ International adverse electronic and physical media searches ☒ English and foreign language data sources ☒ Other relevant industry sources

Data is assessed using a built-in screening platform provided by World-Check.


7. Data Subject Individual Rights

The GDPR provides the following rights for individual data subjects:

- ☒ The right to be informed
- ☒ The right of access
- ☒ The right to rectification
- ☒ The right to erasure
- ☒ The right to restrict processing
- ☒ The right to data portability
- ☒ The right to object
- ☒ Rights in relation to automated decision making and profiling.

7.1 Right to be informed

Data Subjects have the right to be informed about the collection and use of their personal data which is a key transparency requirement under the GDPR.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

The Company provides individuals with information including, the purpose for processing their personal data, the retention periods for that personal data and who it will be shared with, collectively known as the Privacy Notices.

Privacy Notices are provided to individuals at the time the personal data is collected from them and within 1 month when personal data is obtained from other sources. In some instances, the Privacy Notices are not provided, and this is usually the case when the individual already has access to the information. The Privacy Notices are concise, transparent, intelligible, easily accessible and is disseminated in clear and plain language.

The DPO regularly reviews, and where necessary, updates the Privacy Notices specially to bring new uses of individual's data to their attention before processing begins.

7.2 Right of access

Data subjects have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

The DPO reserves the right to refuse to grant a data subject access if it is determined that the request is manifestly unfounded or excessive. The DPO will confirm in writing to the Board of

Directors if he/she believes that the data request is not justified setting out the reasons as soon as practical. The Board of Directors will review the justification of the DPO to reject the data access request and will provide a final decision. The DPO will require approval from the Board of Directors before confirming to the data subject if the data access request has been refused.

Where the DPO approves a right to access, he/she shall liaise with all relevant departments who hold the data, for the purposes of gathering all data related to the request for access. The DPO may request The Company's IT providers to make a search of documentation on The Company's systems who will provide a copy of all data to the DPO.

Should there be a delay whereby the Company will not be in a position to provide the data within 1 month, the DPO will write to the data subject to confirm any delays and advise the reasons for same.

Data will be provided to the data subject by way of:


1. Hard copy format or
2. Digital format by electronic means.

Data Subjects are informed of their right to access their personal data and may be provided a supplementary form to fill, in order to facilitate their request.

7.3 Right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. Any individual can make a request for rectification verbally or in writing to The

Company, and details of where such request should be made are provided to the data subjects in the Privacy Notices. Data subjects may be provided supplementary forms to fill, in order to facilitate their request.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

The Company responds to all requests within 1 calendar month, and may, only in certain circumstances refuse a request for rectification. A copy of the amended data will be provided by the

DPO to the data subject confirming that the data has been amended or completed if deemed as being incomplete.

Should there be a delay whereby the Company will not be in a position to provide the data within 1 month, the DPO will write to the data subject to confirm any delays and advise the reasons for same.

Data will be provided to the data subject by way of:

1. Hard copy format or
2. Digital format by electronic means.

7.4 Right to erasure

The GDPR introduces a right for individuals to have personal data erased also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances/lawful bases.

Data subjects are able to make a request, if applicable, to the Company either verbally or in writing.

The Company will respond to all requests within 1 month.

A determination to erase data will be based on the following criteria:

- The data is no longer necessary for the purpose it was collected;
- The data subject withdraws consent;
- There are no legitimate grounds to process the data;
- There is no legal obligation to continue to store the data;
- The data has been unlawfully processed; and
- To comply with GDPR or other legislation.


If a decision has been made by the DPO to grant the data subject's request for erasure, they will inform the data subject of this fact.

7.5 Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data, however this is not an absolute right and only applies in certain circumstances/lawful bases. When processing is restricted, the Company is permitted to store the personal data, but not use it. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Data subjects are able to make a request, if applicable, to the Company either verbally or in writing.

The Company will respond to all requests within 1 month.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

7.6 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

International Data Transfers – Schrems II Compliance

Following the Court of Justice of the European Union’s Schrems II ruling (C-311/18, July 2020), the Company has reviewed all third-country data transfer arrangements. Where personal data is transferred outside the EEA, the Company relies on the European Commission’s Standard Contractual Clauses (2021 version) and conducts Transfer Impact Assessments to evaluate the level of data protection in the receiving country.

The Company maintains a data transfer mapping register identifying all third-country processor relationships, the legal basis for each transfer, and the supplementary measures in place. All legislative references in this Policy should be read as references to enacted Cyprus legislation (Law 125(I)/2018) transposing the GDPR.

Data Subjects are required to fill in a ‘Data Transfer Form’, providing details of the third party to whom they wish the data sent and must ensure that they provide permission for such a transfer to take place.

7.7 Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

7.8 Rights related to automated decision-making including profiling

The GDPR has provisions on:


- automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if the Company are carrying out solely automated decision-making that has legal or similarly significant effects on them.

The Company can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or authorised by Union or Member state law applicable to the controller; or based on the individual’s explicit consent.

Currently the Company utilises decision making and profiling in order to ascertain if a client of the

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

Company is appropriate to trade in the products offered by the Company or receive services. The 'Appropriateness Test' and 'Suitability Requirement' obligations stem from the Company's requirements under the governing law to create a risk, economic and appropriateness profile on their clients.

8. Accountability and governance

The Company has implemented appropriate technical and organisational measures that ensure and demonstrate its compliance with the GDPR. This include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

Further to this, the Company maintains relevant documentation on processing activities including, but not limited to its Information Asset Register, Data Flow Maps and Data Protection Policies. It has also implemented measures that meet the principles of data protection by design and data protection by default which includes:

- ☒ Data minimisation
- ☒ Transparency
- ☒ Creating and improving security feature on an ongoing basis
- ☒ Allowing individuals (including external auditors) to monitor processing and processes
- ☒ Use Data Protection Impact Assessments (DPIA) where appropriate
- ☒ Having in place written contracts with processors ensuring clarity as to both parties' responsibilities and liabilities
- ☒ Documenting of processing activities and maintaining adequate records
- ☒ Implementation of information audits or data-mapping exercises

9. Data protection impact assessments

A data protection impact assessment (DPIA) is a process which helps the Company identify and minimise the data protection risks of a project/process. DPIA must be carried out for certain listed types of processing, or any other processing that is likely to result in high risk to individual's interests.

The DPIA must:

- ☒ describe the nature, scope, context and purposes of the processing;
- ☒ assess necessity, proportionality and compliance measures;
- ☒ identify and assess risks to individuals; and
- ☒ identify any additional measures to mitigate those risks.


To assess the level of risk, the Company considers both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The DPIA will be carried out by the DPO.

9.1 DPIA Process

The Company will always carry out a DPIA when:

- ☒ Using systematic and extensive profiling or automated decision-making to make significant decisions about data subjects;

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

- ☒ Processing special categories of data or criminal offense data on a large scale;
- ☒ Using new technologies;
- ☒ Using profiling, automatic decision making or special category data to help make decisions on a data subjects' access to a service/product;
- ☒ Processing biometric or genetic data;
- ☒ Processing personal data without providing a privacy notice directly to the data subject;
- ☒ Processing personal data which could result in a risk of physical harm in the event of a security breach;

The Company will consider carrying out a DPIA when:

- ☒ Automated decision-making with significant effects;
- ☒ Processing of sensitive data or data of a highly personal nature;
- ☒ Processing on a large scale;
- ☒ Processing of data concerning vulnerable data subjects;
- ☒ Innovative technological or organisational solutions;
- ☒ Processing involving preventing data subjects from exercising a right or using a service or contract;


When carrying out a DPIA, the Company will:

- ☒ Describe the nature, scope, context and purpose for the processing;
- ☒ Ask any data processors to help us understand and document their processing activities, thereby identifying any associated risks;
- ☒ Ensure that the processing is necessary for and proportionate to the Company's purposes, describing how the Company's will ensure data protection compliance;
- ☒ Make an objective assessment of the likelihood and severity of any risks to individuals' rights and interests;
- ☒ Identify measures the Company can put in place to eliminate or reduce high risks;
- ☒ Record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- ☒ Implement the measures identified and integrate them into our project plan.
- ☒ Keep DPIAs under review and revisit them if necessary.

10. Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The Company takes reasonable precautions to protect personal information/data from loss, theft, misuse, unauthorized access or disclosure, alteration, or destruction. The Company employs physical, electronic, and procedural safeguards to protect personal information/data and it does not store personal information/data for longer than necessary for the provision of services or as permitted by law.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

The Company's datacenter(s) contain both internal and external servers. Access to the Company's internal server is restricted to authorised personnel (i.e. employees and authorised serviceproviders), servers and locations; our external servers can be accessed via the Internet. Any personal information/data provided by clients to the Company will be strictly protected under enhanced measures of security, protected against loss, misuse, unauthorized access or disclosure, alteration, or destruction with use various security measures such as encryption during data transmission, strong authentication mechanisms and separation of machines and data to provide secure areas in order to protect clients' personal information from unauthorised users and such personal information will be treated as confidential and shared only with the Company and its affiliates and/or authorised service providers and shall not be disclosed to any third parties except, and without notice, in accordance with the provisions of this Policy as well as under any regulatory or legal proceedings.

The Company also informs all clients to serve and protect their personal data and advises all clients to maintain confidentiality and not share with others its usernames and passwords provided by the

Company. The Company bears no responsibility for any unlawful or unauthorised use of clients' personal information due to the misuse or misplacement of clients' access codes (i.e.passwords/credentials), irrespective of the way such use was conducted including without limitation negligent or malicious use.


The Company uses reasonable endeavours to implement appropriate policies, rules and technical measures to protect the personal data that we have under our control (having regard to the type and amount of that data) from unauthorised access, improper use or disclosure, unauthorised modification, unlawful destruction or accidental loss. For instance, our security measures include, but are not limited to:

- ☒ educating our employees as to their obligations with regard to your personal data;
- ☒ requiring our employees to use passwords and two-factor authentication when accessing our systems;
- ☒ encrypting data sent from your computer to our systems during internet transactions and client access codes transmitted across networks;
- ☒ employing firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses entering our systems;
- ☒ using dedicated secure networks or encryption when we transmit electronic data for purposes of outsourcing;
- ☒ practicing a clean desk policy in all premises occupied by us and our related bodies corporate and providing secure storage for physical records; and ☒ employing physical and electronic means such as alarms, cameras and guards (as required) to protect against unauthorised access to buildings.

The Company ensures that data subject's information will not be disclosed to government institutions or authorities except if required by law (e.g. when requested by regulatory bodies or law enforcement organisations in accordance with applicable legislation).

10.1 IT Department

The company requires that all computer equipment is connected to a Firewall, anti-malware software, and automatic updating facilities that are all up to date and meet the corporate minimum business standards acceptable in the financial industry. The company also requires:

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

☒ deployment of the corporate policy on usernames and passwords, to have a password protected screensaver, and to password protect and encrypt all folders containing confidential corporate information, sensitive personal information, personally identifiable information, and to disable folder and printer sharing.

☒ All notebook computers that carry personal data or are able to connect to systems that store or process personal data, use full-disk encryption.

☒ that notebook computers are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft.

☒ That the IT departments ensures that all the recent operating system and application security-related patches, fixes and updates have been installed.

☒ Employees to comply with the corporate requirements on the means of connecting to public access points and accessing corporate information.

☒ That all computers and notebooks are protected by an anti-virus and antimalware software.

11. Personal data breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Company is obliged to do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, The Company is required to also inform those individuals/data subjects without undue delay.

The below procedures are there to provide a framework for reporting and managing data security breaches affecting personal or sensitive data held by the Company.

A personal data breach is defined as having the potential to affect the confidentiality, integrity or availability of personal data held by the Company in any format. Such breaches may happen for any number of reasons including:

- ☒ The disclosure of confidential data to unauthorised persons;
- ☒ Loss or theft of data and/or equipment on which data is stored;
- ☒ Inappropriate controls allowing for unauthorised use of information;
- ☒ Breaches in the Company's IT systems and security;
- ☒ Unauthorised access to computer systems e.g. hacking;
- ☒ Viruses or other security attacks;
- ☒ Breaches of physical security where data is kept;
- ☒ Leaving IT equipment unattended allowing unauthorised access;
- ☒ Emails containing personal data sent in error to the wrong recipient.

11.1 Breach Detection and Internal Reporting

Where a privacy data breach is known to have occurred (or is suspected) any member of the

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

Company staff who becomes aware of this must, within 24 hours, alert the DPO via email. The information that should be provided to the DPO by the relevant staff member includes:

- ☒ When the breach occurred (time and date);
- ☒ Description of the breach (type of personal information involved);
- ☒ Cause of breach (if known) and how the breach was discovered;
- ☒ Extent of the breach (how many individuals are affected);
- ☒ Which systems, if any, have been affected;
- ☒ Whether any corrective actions/measures have been taken to remedy the breach (or suspected breach)

11.2 Investigation

Once notified of the suspected or potential breach, the DPO must investigate and establish if a data breach has occurred, or is likely to have occurred, and assess the level of severity. The following criteria may be used by the DPO to assess if a breach has occurred:

- ☒ Whether personal data is involved;
- ☒ Whether the personal data is of a sensitive nature;
- ☒ Whether there has been unauthorised access to personal information, or unauthorised disclosure of personal data or loss of data where access is likely to occur.

The following criteria can be used to assess the severity of the data breach:

- ☒ The type and extent of personal information breached;
- ☒ Whether multiple individuals have been affected;
- ☒ The persons or type of persons who now have access to the data;
- ☒ Whether there is (or could be) a real risk of serious harm to the affected individuals, which could include, but is not limited to, physical, physiological, emotional, economic/financial or harm to reputation;

Depending on the outcome of the above investigation, the DPO will issue immediate remedial instructions to manage the data breach, depending on the nature and severity. This may include ensuring that immediate corrective action is taken, if this has not yet occurred. Such action may include retrieval or recovery of data, ceasing unauthorised actions or shutting down/isolating the affected system;

11.3 Breach Reporting and Notification

Where it is confirmed by the DPO that there is a reportable breach of the GDPR, unless the data was anonymised or encrypted, the DPO will immediately write to the relevant competent authority within 72 hours or as soon as practicable of the identified breach. Notification will include:

- ☒ The specific breach of the GDPR;
- ☒ How the breach was identified;
- ☒ The impact on the data subject and any other data subjects;
- ☒ Action being taken to remedy the breach; and

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

Any request for advice on further actions.

The DPO may decide, depending on the severity of the breach and the potential harm it may cause the data subject, to make notification to the affected data subjects. Such notification will likely include:

- Nature of the breach of the GDPR;
- The contact details of the DPO or his/her alternate;
- Potential consequences of the data breach; and,
- Action being taken by the data controller to take corrective action.

The DPO will not contact the data subject if it is determined that:

- The Company has implemented appropriate technical and organisational protection measures that render the personal data unintelligible to any person who is not authorised to access it;
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects are not affected: and, It would involve a disproportionate effort.

Following this notification, the DPO will ensure to identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence, this may include a review of policies, processes and/or refresher training.

11.4 Record Keeping

The Company will maintain a Data Breach Register which will include the following information:

- Date of breach;
- Nature of breach;
- Impact on data subject;
- Is it a reportable event to the ICO;
- Is it a reportable event to the data subject;
- Action taken to resolve.


The Company will document all potential breaches regardless of whether a decision to report the breaches is made.

The responsible person for managing breaches will lie with the Company's DPO who in turn will ensure sufficient training of the Company's staff. The Company staff must be aware of how to escalate security incidents to the DPO.

12. Training

The DPO or his/her alternate will provide training on an annual basis or as required to all employees in accordance with GDPR.

A signed attendance log will be retained by the DPO as evidence of attendance by employees.

	DATA PROTECTION POLICY	
	MARCH 2026	V2.1

13. Payment Credential Data Retention

Payment card credentials (including tokenised card data and payment instrument references) shall be retained for the minimum period necessary to perform the services for which they were provided, and in any event for no longer than 3 months following the last successful transaction. Upon closure or termination of a Client account, all stored credentials shall be purged within [30/60] calendar days.

14. PCI DSS Compliance Framework

In addition to GDPR compliance, the processing of cardholder data is subject to the Payment Card Industry Data Security Standard (PCI DSS). The Company and its authorised payment processors maintain PCI DSS compliance. The Company does not store full Primary Account Numbers (PAN), CVV2/CVC2 codes, or magnetic stripe data. The Company retains Attestations of Compliance (AOC) from each payment processor engaged.

15. Cross-Border Data Transfer Safeguards

The Company identifies the following specific legal safeguards for international data transfers: (a) for transfers to jurisdictions with an EU adequacy decision, reliance on that decision; (b) for all other transfers, Standard Contractual Clauses (SCCs) under GDPR Article 46(2)(c), supplemented by Transfer Impact Assessments where required.

Third-party processor agreements include data localisation provisions and audit rights. A detailed register of international transfers, identifying each processor, jurisdiction, and applicable safeguard, is maintained by the Data Protection Officer.