Data Privacy Policy

Important Information

In line with Article 24 GDPR (EU) 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, APM has implemented appropriate technical and organisational measures to ensure compliance with, and pursuance to, the General Data Protection Regulation (GDPR). This policy stands as the cornerstone of APM compliance with GDPR and is reviewed and updated accordingly.

1. General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organisations across the region approach data privacy.

In line with Article 5 of GDPR, APM must conform to the following principles at all times.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with GDPR.

APM is at all times responsible for, and able to demonstrate compliance with the aforementioned principles.

2. Applicability

This privacy policy applies to the processing activities of APM. The details of APM are as follows:

APM Capital Markets Limited: a company registered in England and Wales under register number 03148972. The registered address of the company is 1st Floor, 7-10 Chandos Street, London, W1G 9DQ United Kingdom. It is registered with the UK Information Commissioner under registration number is Z1457804.

APM provides execution only trading services to retail and professional clients for Spread Betting ('SB') and Contract for Difference ('CFD') products.

3. Compliance Monitoring

In order to maintain a high level of compliance in relation to the rules stipulated within this policy, APM carries out an annual Data Protection compliance audit. Conducting a thorough diagnostic audit allows APM to recognise any deficiencies or areas for improvement; upon mitigation, ensuring total compliance to GDPR. Examples of the areas covered within an audit include:

- Data protection governance, and the structures, policies and procedures to ensure GDPR compliance;
- The processes for managing both electronic and manual records containing personal data;

- The processes responding to any request for personal data;
- The technical and organisational measures in place to ensure that there is adequate security over personal data;
- The provision and monitoring of staff data protection training and the awareness of data protection; and
- Data audit as per Appendix 2.

4. Data Subject Rights and Requests

GDPR provides the following rights for individuals:

- 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; and
- Rights in relation to automated decision making and profiling.

APM has in place adequate systems and controls to enable and facilitate the application of the eight data subject rights listed above.

When a data subject makes a request, APM will embark on a pragmatic decision-making process headed up by the Data Protection Officer.

Unless APM deems requests to be excessive or unnecessary in their nature, no fee will be charged to the data subjects for considering and/or complying with such requests.

5. Rights to Access

All requests of this nature should be referred to the Data Protection Officer. APM shall respond to such requests within 30 days.

The data subject has the right to obtain the following information from APM:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of personal data stored for the data subject;
- The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; and
- The use of any automated decision-making e.g. profiling.

When requested, APM shall provide a copy of the personal data held. For any further copies requested by the data subject, APM may charge a reasonable fee based on administrative costs. Where requests are made via electronic means, APM shall provide the data in a commonly used electronic form.

6. Right to Rectification

APM shall ensure all that data subjects are able to exercise their right to obtain from the firm, without undue delay, the rectification of inaccurate personal data concerning him or her.

7. Right to Erasure

Without undue delay, APM shall erase personal data of a data subject where requested, and where one of the following grounds applies:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- The data subject withdraws consent which the processing is based on, and where there is no other legal ground for the processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or where the data subject objects to processing;

- The personal data has been unlawfully processed;
- The personal data has to be erased compliant with a legal obligation in the member state law; and/or
- The personal data has been collected in relation to the offer of information society services.

Article 17 3 (b) GDPR, states that the right to erasure is disapplied where the firm must retain data in order to comply with other applicable regulation. The superseding regulations in APM case are The Money Laundering Regulations requirement for firms to hold KYC data for 5 years, and MiFID II Article 16 requirements on record keeping. This is referred to in APM privacy notice.

8. Right to Restrict Processing

APM will cease the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, APM will restrict the processing until the accuracy of the data is verified;
- Where an individual has objected to the processing and APM is considering whether it has legitimate grounds to override those of the individual;
- When processing is found to be unlawful and the individual opposes erasure and requests a restriction instead; and/or
- If APM no longer needs the data but the individual requires the data to establish, exercise or defend a legal claim.

9. Right to Data Portability

The right to portability only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

To comply, APM must:

- Provide the personal data in a structured, commonly used and machine readable format;
- Provide the data free of charge (unless excessive or unnecessary);
- If requested and technically feasible, transmit the data directly to another organisation; and
- Consider possible prejudice of the rights of individuals, where the personal data concerns more than one individual.

10. Consent

Consent must be given by a clear affirmative act, which establishes freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their data. APM will obtain consent via a written statement, by electronic means, or an oral statement.

APM requests, manages and records consent pursuant to Articles 5, 6, 7 and 9 of GDPR.

- APM checks that consent is the most appropriate lawful basis for processing;
- APM makes the request for consent prominent and separate from its terms and conditions;
- APM requests a positive opt in;
- APM does not use pre-ticked boxes or any other type of default consent;
- APM uses clear, plain language that is easy to understand;
- APM specifies why it wants the data and its purpose;
- APM provides granular options to consent separately to different purposes and types of processing;
- APM names its organisation and any third party controllers who will be relying on its consent;
- APM ensures that individuals can refuse to consent without detriment; and
- APM avoids making consent a precondition of service.

APM records when and how the firm obtained consent from individuals. The firm also keeps a record of the exact information originally provided.

Exercises APM may carry out to ensure the appropriate management of consent include the following:

- APM regularly reviews consents to check that the relationship, the processing and the purposes have not changed;
- APM has processes in place to refresh consent at appropriate intervals, including any parental consents (if so applicable);
- APM considers using privacy dashboards or other preference-management tools as a matter of good practice;
- APM makes it simple for individuals to withdraw their consent at any time, and publicises how this is done;
- APM acts on withdrawals of consent as soon as possible; and
- APM does not penalise individuals who wish to withdraw consent.

APM will not infer consent from silence or inactivity. When the processing of personal data has multiple purposes, APM will obtain consent for all of these. Where a data subject's consent is to be given following a request by electronic means, APM will ensure the request is clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

11. Data Privacy by Design

APM has in place technical and organisational measures which integrate data protection into processing activities.

Privacy and data protection is a key consideration in the early stages of any project APM undertakes

For example, when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative; and/or
- Using data for new purposes.

Privacy and data protection considerations will be integrated within APM risk management methodologies and policies.

12. Data Protection Impact Assessments (DPIA)

APM carries out a DPIA where data processing is likely to result in high risk to individuals, for example:

- Where a new technology is being implemented;
- Where a profiling operation is likely to significantly affect individuals; and/or
- Where there is large scale processing of special categories of data.

In assessing the level of risk, APM considers both the likelihood and severity of any impact to the individuals concerned.

APM ensures that there is a sound understanding of DPIA amongst certain members of the firm.

- APM provides training so that all staff understand the need to consider a DPIA at the early stages of any plan involving personal data;
- APM existing policies, processes and procedures include references to DPIA requirements, where applicable;
- APM understands the types of processing that requires a DPIA;
- APM creates and documents a robust DPIA process; and
- APM provides training for relevant staff on how to carry out a DPIA.

13. Breach Reporting

In the case of a personal data breach, APM shall without undue delay, and where practicable, notify the relevant supervisory authority not later than 72 hours after having become aware of the breach. This is not required where the breach will not likely result in a risk to the rights and freedoms of natural persons.

Where the notification is not made within 72 hours, APM must provide a valid reason for the delay. Relevant supervisory authorities contact details can be found within Appendix 1.

Notifications made by APM shall at least:

- Describe the nature of the personal data breach;
- Communicate the name and contact details of the relevant department handling the data breach;
- Describe the likely consequences of the personal data breach; and
- Describe the measure taken or proposed to be taken by APM to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of subjects, APM shall communicate the data breach to the data subject without undue delay.

APM shall communicate the matter to the data subject in clear and plain language the nature of the personal data breach, detailing at least the information in points (b), (c) and (d) as above.

14. Record Keeping

APM employs fewer than 250 people and therefore Article 30 GDPR is technically not applicable. That being said, due to the other data monitoring requirements dictated by GDPR and for best practice, APM shall maintain a record of processing activities under its responsibility. That record shall contain the following information:

- The name and contact details of the controller;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The recipients to whom the personal data has been or will be disclosed including recipients in third counties or international organisations;
- Where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation;
- Where possible, the envisaged time limits for erasure of the different categories of data; and
- Where possible, a description of the technical and organisation measures referred to in Article 32(1).

APM keeps records in writing, and in electronic format.

If requested by the relevant supervisory authority, APM will make records available immediately.

15. Complaints Handling

Upon receipt of a data subject complaint, APM shall internally investigate the complaint. APM shall inform the data subject of progress and subsequently the outcome of the complaint. This must be communicated within a reasonable period.

Where the complaint cannot be resolved between the data subject and APM, the data subject may choose to seek redress through mediation, litigation procedure or via a complaint to the supervisory authority. APM must inform data subjects of their right to complain directly to the relevant supervisory authority.

16. Appendix 1

Personal data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person
Data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data subject	The identified or identifiable natural person to which the data refers
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
International organisation	An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Supervisory Authority	Data protection supervisory authority for APM Capital Markets Limited: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel: +44 (0) 303 123 1113 Fax: +44 (0) 1625 524 510 Website: www.ico.org.uk

17. Appendix 2

Monitoring Data checklist

Details of the data held by APM	
Reason for holding the data	
Methods for obtaining the data	
Date that the data was obtained	
Individuals responsible for the data	
Data storage	
Data retention	
Data deletion methodology	