Apex CB Financial Planning Ltd

DATA PROTECTION POLICY

1. INTRODUCTION

The Company holds and processes information about employees, clients, and other data subjects for commercial purposes. When handling such information, the Company, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (the Act). In summary these state that personal data shall:

1. be processed fairly and lawfully,
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose,
3. be adequate, relevant and not excessive for the purpose,
4. be accurate and up-to-date,
5. not be kept for longer than necessary for the purpose,
6. be processed in accordance with the data subject's rights,
7. be kept safe from unauthorised processing, and accidental loss, damage or destruction,
8. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.
9. exclude data held in publically accessible sources.

2. LEGAL BASIS FOR PROCESSING

Data will be processed by the firm on the following legal bases:
(a) Consent: the individual has given clear consent for us to process their personal data for the purpose of providing financial advice and ongoing management of their financial contracts and services.
(b) Contract: the processing is necessary for contracts we administer on behalf of the individual, or because they have asked us to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

3. DEFINITIONS

"Staff" means employee of Apex CB Financial Planning Ltd.
"Employees" and **"other data subjects"** may include past, present and potential members of those groups.
"Other data subjects" and **"third parties"** may include contractors, suppliers, contacts, referees, friends or family members. **"Processing"** refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.
"Client" or **"Clients"** means past, present or potential customer(s) of Apex CB Financial Planning Ltd.

4. NOTIFICATION OF DATA HELD

The Company shall notify all staff and other relevant data subjects of the types of data held and processed by the Company concerning them, and the reasons for which it is processed. When processing for a new or different purpose is introduced the individuals affected by that change will be informed and the Appendix 1 will be amended.

5. STAFF RESPONSIBILITIES

All staff shall:
• ensure that all personal information which they provide to the Company in connection with their employment is accurate and up-to-date;
• inform the Company of any changes to information, for example, changes of address;
• check the information which the Company shall make available from time to time, in written or automated form, and inform the Company of any errors or, where appropriate, follow procedures for updating entries on computer forms. The Company shall not be held responsible for errors of which it has not been informed.

When staff hold or process information about clients, colleagues or other data subjects they should comply with GDPR guidelines.

Staff shall ensure that
- all personal information is kept securely;
- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. *Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.*

6. RIGHTS TO ACCESS INFORMATION

Staff and clients of the Company have the right to access any personal data that is being kept about them either on computer or in manual files. Any person may exercise this right by submitting a request in writing to the Directors.

Before proceeding with the subject access request we must verify the identity of the data subject making the request, in line with our identity verification procedures.

The Company will not charge for Subject Access Requests. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee is likely to be based upon time spent using the hourly rates set out in our standard terms.

The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month. We may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the data subject within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where we refuse to respond to a request, we will explain why to the data subject, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

7. RIGHT TO BE INFORMED

As our data is entirely obtained directly from our clients (the data subjects) our data protection procedures and client agreement provide the identity and contact details of the data controller and data protection officer. They also set out the purposes of processing and our legitimate interests, and inform clients that their data may be passed on to legitimate 3rd parties such as for the process of application for financial products and services.

Client will be informed at the point of data collection that the failure on their part to provide full, complete and relevant information will impact upon the scope and quality of advice given.

8. THE RIGHT TO RECTIFICATION

Should a client inform us that their data is inaccurate we will undertake to amend the data and confirm with them that it accords with their understanding within one month. This may be extended by two months where the request for rectification is complex.

Where we are not taking action in response to a request for rectification, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

9. THE RIGHT TO ERASURE ('THE RIGHT TO BE FORGOTTEN')

Where a subject requests that their data should be erased it will be necessary to identify whether any of this data must be retained for the necessary processing of their financial products and services, and to provide evidence of advice given to the subject to the regulator, or for the exercise or defence of legal claims. Where data is held to comply with legal (regulatory) purposes such requests will be declined. Once we have identified which data can be erased this will be confirmed to the client in writing.

10. THE RIGHT TO DATA PORTABILITY

Where a subject request that data be transferred to another provider we will contact the Data Processor (the provider of the firm's database) and request that this be provided in a machine readable form (e.g. CSV). Such requests must be completed within one month. This can be extended by two months where the request is complex or we receive a number of requests. We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

Where we are not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

11. THE RIGHT TO OBJECT:

All clients will be explicitly informed of their right to object "at the point of first communication" (usually the first meeting) and in our Privacy Notice.

Where a client objects to processing their data based on legitimate interests of the performance of the task in the exercise of official authority, this potentially conflicts with our conduct of business requirements set by the Financial Conduct Authority and they must be informed of this.

Should a client object to direct marketing then we must immediately cease all forms of direct marketing communication, and ascertain whether it relates to communication via a certain medium or all marketing communications. Our database must be updated to reflect this selection of the relevant tick boxes on the details tab, and our standard process is to add the words "DO NOT CONTACT" in line one of their address as a failsafe.

12. RIGHTS TO AUTOMATED DECISION AND PROFILING

None of the data that we collect and process is automatically profiled or decisions made on an automated basis. For example use of the investment risk profiling tool that produces a report based on questions answered by the client. However this is manually reviewed by the adviser and the risk profile is selected based upon recommendations from the profiling software. The adviser is expected to use information collected through discussion with the client in order to select an appropriate risk profile that meets their needs and objectives.

13. SUBJECT CONSENT

In some cases, such as the handling of sensitive information, the Company is entitled to process personal data only with the consent of the individual.

14. SENSITIVE INFORMATION

The Company may process sensitive information about a person's health, disabilities, criminal convictions, or financial information.

The Company also asks for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The Company will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency.

15. THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLERS

The Company is the data controller under the Act, and the Managing Director is ultimately responsible for implementation. Information and advice about the holding and processing of personal information is available from the Directors.

16. THIRD-PARTY DATA PROCESSORS

Where client data is input onto third-party systems, such as the back office and provider quotation and product application systems the Company will maintain an up to date written contract.

17. RETENTION OF DATA

The Company will keep different types of information for differing lengths of time, depending on legal and operational requirements. Data collected for the purposes of providing regulated financial advice and/or services will be held indefinitely.

18. COMPLIANCE

Compliance with the Act is the responsibility of all members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings.

Any individual, who considers that the policy has not been followed in respect of personal data about him- or herself, should raise the matter with the Directors initially. If the matter is not resolved it should be referred to the staff grievance procedure.

Policy approved by

Signature	
Date	**23/11/2020**
Print Name	Christopher Ryan