Quilter Financial Planning

Data Protection Policy

Guidance Owner: Data Guardian
Version: 2.0

Quilter Financial Planning

Contents

Introduction

Quilter Financial Planning ("QFP") is a financial services distribution network. Through its network of Appointed Representative (AR) Firms and Advisers, QFP provides UK consumers with access to products and services from financial services companies, covering the entire spectrum of financial advice.

As a company, QFP is committed to dealing with our AR firms, customers and employees with honesty and integrity. As part of this commitment, we will make every effort to ensure that all Personal Data is handled in accordance with the relevant Data Protection Law. Our policy framework sets out the necessary requirements and principles to manage and mitigate key risks and ensure compliance with Data Protection.

QFP acknowledges that its business is underpinned by personal data, which is an important business asset and therefore must be kept secure, both to preserve the privacy of individuals and to safeguard QFP's reputation. QFP will therefore take all steps necessary, to ensure that it adheres to the requirements of the Data Protection Regulation.

This document is the Data Protection Policy (the "Policy") for QFP and forms part of the wider Policy and Standards framework which forms the Quilter Group Governance Manual ("GGM"). This Policy compliments the Personal Data Privacy Policy which is the Policy that applies to all parts of the Quilter group. Where any instruction in this policy conflicts with the Personal Data Privacy Policy then the Personal Data Privacy Policy shall take precedence.

This policy sets out QFP's approach to how it collects, processes, manages, transfers, discloses, retains and destroys any personal data either controlled or processed by QFP, including the personal data of its employees.

This document should not be read in isolation. This policy is supported by a number of Standards and Guidance documents that provide more detail on the requirements. These guidance documents are included in the appendices. This policy is also linked to other policies which are listed in the appendices.

Context

Data Privacy and security is a key area of regulatory focus and an expectation for all customers, clients and employees who share personal data with QFP. In this context QFP and AR member firms are required to implement robust technical and organisational controls to protect personal data, in all its forms processed by or on behalf of QFP.
Data Privacy controls should be proportionate to the Data Protection risks, relevant to QFP's data processing activities, to ensure the appropriate balance between cost and risk mitigation. It is therefore important for the business to set the priorities for safeguarding privacy.

This Policy

Policy Objective

The objective of this policy is to ensure everyone in QFP, including AR member Firms, understands their obligations to comply with the relevant Data Protection Law in order to:

- Assure the data privacy of customers, staff, advisers and other individuals who interact with QFP and AR firms
- Mitigate against specific information risks
- Ensure compliance with the relevant Legislation

Scope of Policy

This Policy applies to all processing of personal data by QFP, Member (AR) Firms, Advisers and Employees and any 3rd party suppliers of services to QFP, where 'processing' includes any operation undertaken on the data, including receipt, use, storage and disposal.

Employees are defined as "permanent and fixed term contract employees engaged under a contract of employment or Executive Service Agreement and the following categories of individuals who provide services to or on behalf of the firm; Non-Executive Directors, temporary staff engaged via an agency, contractors (e.g. self-employed) engaged via a limited company or similar".

Member firms are defined as "AR firms, Registered Individuals, trading styles, self-employed advisers and any further individuals who are engaged in the giving of advice as part of the QFP network".

The Policy applies to data held in any format (electronic or hard copy/paper) or system, or processed by any means.

Policy Owner and Review

This policy is analogous to the Quilter Personal Data Privacy Policy is the responsibility of the Group Policy Owner ("Group Policy Owner"). The QFP Data Guardian will be appointed as the QFP Policy owner.

The QFP Data Guardian is responsible for monitoring that this policy is, and remains, effective by seeking reasonable assurance that the relevant risks have been identified and assessed and that the relevant controls, and other mitigating actions, are adequately designed and operating effectively.

On a half-yearly basis, the QFP Policy Owner is expected to attest to the Group Data Protection Officer ("GDPO") that their Business is in compliance with the requirements of this Policy and the Quilter Personal Data Privacy Policy, must be able to provide suitable evidence to prove this.

Exceptions

This Policy is effective from 25th May 2018, and subject to review in the event of a significant change to the business impacting this policy.

Areas where the requirements set out in this Policy are perceived to be in conflict with legal and regulatory requirements applicable at Business level must be communicated to the QFP Data Guardian whomay escalate to GDPO or to the Group Policy Owner.

Definition of Personal Data

Personal data means *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

What is a Data Privacy Risk?

Data Privacy Risk affects all personal data relating to all QFP Member (AR) Firms, Advisers, Clients and Employees and any contractors or 3rd party suppliers of services to QFP.

The Data Privacy Risk is defined below as:
"The risk that personal data is not sufficiently secure or in not processed in accordance with legislative requirements with potential to cause detriment to individuals, resulting in financial loss, damage to reputation and / or regulatory fines/censure."

Data Protection Principles and Requirements

Data Protection Law establishes a framework of rights and duties which are designed to safeguard personal data. This framework aims to balance the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect the privacy of their personal details.

Data Protection governs the collection, storage, use and disclosure of personal data, setting high standards that data controllers and data processors must adhere to when processing personal data. Therefore, QFP as controller and/or processor of personal data must ensure that it takes appropriate measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Information Commissioner's Office (ICO) is the independent Supervisory Authority in the UK, responsible for upholding information rights in the public interest. The ICO sets out guidance on the obligations of firms to meet Data Protection and Information Security obligations. QFP is required to cooperate, on request, with the ICO in the performance of its tasks.
More detailed information about Data Protection Law can be found by reading the Information Commissioner's Office guide which can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-Regulation-gdpr/.

The Principles

Data Protection is underpinned by a number of principles which drive compliance:

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 they are 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 datasubjects for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriatesecurity of the personal data, including protection against unauthorisedor 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 the relevant Data Protection Law.

Data Protection Requirements and QFP Guidance

Data Protection Law itself can be complex; however, it is underpinned by the following requirements which ensure that QFP, Member (AR) Firms, Advisers and Employees are able to comply with their Data Protection requirements.

The requirements are emboldened and assigned a unique identifier, for example: Data Privacy Policy requirement number 1 is **DPP 1**.

Underneath each of the requirements is reference to guidance, that supports the DPP, which can be found on the QFP Extranet.

DPP1: AR firms must appoint an appropriately qualified individual who is:

- Fully resourced, independent, without conflicts of interest, and has access to the highest level of management;
- Accountable for monitoring compliance with Data Protection Legislation and this Policy;
- The contact point for Data Protection Supervisory Authorities and data subjects; and
- The lead subject matter expert for privacy matters within their firm.

Information Commissioner's Office Registration Guidance

The requirement to register with the ICO is not a new practice and provision was in place for this within the 1998 Act. This document guides AR firms in complying with the registering of businesses with the ICO in conjunction with the Data Protection Legislation.

Individual with Data Protection Responsibilities Guidance

This document outlines the standards applicable to firms and to clarify the need for a Data Protection Officer (DPO) within AR firms and the roles responsibilities they have. The guidance also provides best practice guidelines and the need to have someone within AR firms who are responsible for Data Protection.

DPP2: Each data controller must:

- Register with the appropriate Supervisory Authority, and pay any fees, as required.
- Nominate, in writing, an EU representative if they are outside the EEA.
- Maintain a register of processing activities that they undertake in a Data Register.

Data Register Guidance

Guidance for AR firms on how to understand the data they hold and create a Data Register. The guidance will provide support and standards for firms on how to document what personal data they hold, where it came from and who they share it with. The Data Register must also identify where all the information is held, what the data is used for, how the information flows through the business, and where data is transferred to 3rd Parties.

DPP3: All processing of personal data must adhere to the Data Protection principles. These records will form part of the evidence that demonstrate the seventh Principle (Accountability):

- Fairness, Transparency and Lawfulness;
- Purpose Limitation;
- Data Minimisation;
- Accuracy;
- Storage Limitation; and
- Confidentiality and Integrity.

This Guidance Document can be used in conjunction with the **Data Protection AR Data Register**, located with the Extranet.

Data Sharing Guidance

This Guidance document provides provision on how AR firms, RI's and QFP can share personal data and the safeguards that should be applied in such circumstances.

Direct Marketing Guidance

This guidance applies to QFP, AR firms, their RI's and any third-party suppliers of marketing services surrounding the action of promoting and selling products or services, including market research and advertising.

Detection of Crime Guidance

This guidance clarifies the impact of the Data Protection Legislation on using any data that is processed that may relate to or indicate a criminal act has taken place.

Deceased Client Information Guidance
This clarifies how the information belonging to deceased clients should be handled, ensuring that this data is handled with the same care and attention as all other clients. Quilter applies the same principles of Data Protection and Information Security to the deceased as it does the living.

Member Firm Adviser Resignations, Dismissals and Disunions Guidance
In the course of business relationships, there are occasions where the structure of a firm may change dramatically, e.g. insolvency, resignations, and creation of competing firms. This document supports AR firms and RI's in ensuring that the client relationships do not suffer as a result and that QFP are kept informed of developments.

Location Guidance
This document provides QFP AR's with guidance surrounding how to remain compliant with the Data Protection Legislation while processing data in a number of differing locations and situations.

Lawful Basis for Processing Guidance
For processing to be Lawful, we need to identify a Lawful basis before we can process personal data as some data subjects' rights will be modified depending on the Lawful basis. The "Lawful basis for Processing Guidance" document outlines the Lawful basis we have for processing data, and provides standards to firms on how to review the types of processing activities they carry out and to identify their Lawful basis for doing so. This will include data processing for both customers and employees.

Data Controller Guidance
The "Data Controller Guidance" document provides an explanation of the data controller responsibilities that are on AR firms and the relationship between QFP and AR firms. It also outlines the data processing activity that falls into joint responsibility and what activity AR firms are solely responsible for.

Special Category Data Guidance
The Special Categories and Criminal Offence Data Guidance outlines the Data Protection requirements with respect to Special Category Data ("SCD") and criminal offences data, and the approach AR firms should take when processing this type of data including how and when they should gather consent to process this information.

Data Retention Policy
Data Retention policy outlines the approach to retaining data with legislative and regulatory requirements.

Data Retention Schedule
The Data Retention schedule presents the period of retention by data type.

Data Disposal Guidance
The disposal guidance document which provides the standards for disposing of data at the end of a retention period and/or when a request is made by a data subject.

Data Management Guidance

Data Management guidance provides support for all areas of good data management including:

- Data Accuracy;
- Data Minimisation;
- Data Sharing – e.g. only sharing it with those you should be sharing it with; and
- Purpose Limitation – e.g. only use data for the purposes it was collected.

Third Party and Supplier Guidance

Guidance on firms' interactions and agreements with 3rd parties.

DPP4: Processes and procedures must be maintained to assure Data Subjects' Rights ("DSR") to be informed, have access to their data, to rectification, to object to or restrict processing, to erasure, to portability, and to not be subject to automated decision-making, in accordance with the criteria set out in Data Protection Law.

Individual Data Rights Policy

The Individual Data Rights (IDR) policy document outlines the increased rights of data subjects which are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to object;
- The right to restrict processing;
- The right to data portability; and
- The right not to be subject to automated decision-making including profiling.

Individual Data Rights Process

The Guidance/Process document provides the process that QFP, employees, AR firms and advisers must follow to adhere to these rights and guidance to allow AR firms to apply the same approach to non-network/non-joint data controller activity and employees that may make a request.

Request for Information from Police and Security Services Guidance

This document outlines the process in which QFP, employees, AR firms and RI's must follow when dealing with a request for information submitted by Police or Security Services (e.g. the Courts), particularly the requirement to report these requests to the Data Guardian's Office at the earliest opportunity.

Data Subject Access Request (DSAR) Guidance

This document is a guideline for how AR firms, RI's and QFP ensure that they hold robust processes to deal with DSARs, including but not limited to a triage process to ascertain whether we have sufficient detail to fulfil the request. Quilter has appointed a Data Guardian who is responsible for the DSAR

process and ensuring that these are dealt within agreed SLA.

In conjunction to the above, see also the DSAR Request Form within the Extranet.

Automated Decision Making and Profiling Guidance

This guidance applies to all QFP AR firms and their RI's, plus any third-party suppliers who undertake automated processing of personal data used to analyse or predict matters relating to an individual (Profiling), and/or decisions made by automated means without any human involvement (Automated Decision Making).

DPP5: Processes and procedures must be maintained to ensure any Data Protection incident is reported to the Supervisory Authority within 72 hours of awareness, where this results in a risk to the rights or freedoms of individuals, and that affected individuals are notified and supported as appropriate.

Data Protection Incident Guidance

Any incident or suspected Data Protection incident must be immediately reported. The Incident Reporting process outlines the approach for AR firms, employees and advisers and provides guidance on what constitutes an Information Security and Data Protection breach.

See also Data Protection Incident Reporting Form on the Extranet.

DPP6: Information about data collection and processing to be provided to data subjects in concise, easy to understand way using clear language

Data Privacy Notice Guidance

Guidance on what information is contained within a Privacy Notice, who needs one and when you need to provide it to clients. The guidance also includes when AR firms need to use a Privacy Notice for non-network clients and employees.

AR Privacy Notice

Privacy Notice to be used by AR firms for their network clients

Verbal Consent Privacy Notice

Privacy Notice to be used by AR firms who conduct their business remotely from their clients (e.g. via telephone) while allowing them to document consent to process data.

AR Internet Privacy Notice

Internet version/summary of Privacy Notice to be used by AR firms for their network clients

AR Corporate Privacy Notice

Privacy Notice to be used by AR firms for their corporate clients

DPP7: Children's personal data should be treated with extra sensitivity and care and additional safeguards put in place when relying on consent to process data

Use of Children's Personal Data Guidance

Although none of the specific scenarios where Data Protection Law requires additional safeguards should form part of our, or our ARs, business, there are some instances where children's data will be gathered. The "Use of Children's Data Guidance" outlines the approach firms and advisers should take to children's data, and the additional procedures that firms should put in place to safeguard this data.

DPP8: Processes and procedures must be maintained to assess the privacy risks of any new data processing activities and to support the aims of Privacy by Default and Privacy by Design.

Data Privacy by Design Guidance

QFP have a general obligation to implement technical and organisational measures to show that we have considered and integrated Data Protection into our processing activities. One of the key ways in which we can demonstrate this is through Data Privacy Impact Assessments ("DPIAs").

The DPIA policy and guidance outlines how and when firms need to apply a DPIA to changes in their business.

Corporate Client Guidance

The Corporate Privacy Notice and guidance recognises that firms who have corporate clients may be undertaking multiples roles and may handle data differently to a standard direct retail client relationship. The Corporate Guidance and Privacy Notice is to help firms meet their obligations with respect to this aspect of their business.

See also **Corporate Client Guidance** and **Corporate Client Guidance Q&As** on the Extranet.

Cooperating with Supervisory Authorities

The Data Protection Legislation provides that the controller (QFP and AR member firms) shall cooperate, on request, with the Supervisory Authority in the performance of its tasks.

Accountability is one of the core principles of Data Protection Law. Data Controllers will need to demonstrate that any processing activities undertaken comply with Data Protection requirements and keep records of those activities to be made available to Supervisory Authorities on request.

Under Data Protection Law, various sanctions can be imposed on firms for a breach of requirements including fines of up to 4% of annual worldwide turnover or EUR 20,000,000, whichever is greater in respect of serious breaches. Firms therefore need to be prepared for the possibility of the ICO taking stricter enforcement action. Sanctions under are required in each individual case to be "effective, proportionate and dissuasive" and will depend on a range of factors including the measures and procedures put in place by the data controller.

This means that firms should be prepared to demonstrate Data Protection compliance upon request from the Supervisory Authorities.

Governance and Oversight

Everyone in QFP, including AR member firms, has a duty to treat all personal data in accordance with

Data Protection Law including a shared responsibility in keeping the data secure to minimise the threat from loss or theft of personal data. The objective of this section is to provide clear ownership and governance for the QFP Data Privacy Policy and supporting guidance and procedures.

QFP Executive

The Executive accept all reasonable obligations in respect of ensuring QFP operate in accordance with Data Protection Law, ensuring the Data Privacy Policy is implemented across the business. This includes Data Protection and Data Security Policies and Procedures and Best Practice Guidance to achieve an effective balance between cost and risk.

Data Guardian/Privacy Office

QFP has appointed Quilter Group to fulfil its obligations to have in place a suitably qualified and experienced Data Protection Officer (DPO). At local level, QFP will have in place a Data Guardian to assist the Data Protection office in their role and to inform and advise local controllers and processors of their obligations under the Regulation. The Data Guardian shall be free of all conflicts of interest with unrestricted access to the group DPO and senior management.

Team Managers

Within QFP, it is the responsibility of the Team Managers to ensure their team adhere to Data Protection Law and that all current and future employees are instructed in their Data Protection responsibilities. This means employees:

- Understand the principles of Data Protection Law and how it affects what they do and haveread and understood policy and guidance in Appendix A that is relevant to them;
- Complete the Data Protection and Information Security training which is mandatory for all employees, including contractors, consultants and those employed through 3rd parties.";
- Are aware of their accountability and that 'wilful' failure to comply or report a potential breach of data is potentially a disciplinary offence which may include action up to and including summary dismissal, following the Disciplinary Procedure in the Quilter EmployeeHandbook.

The team manager Data Protection "checklist" should assist in ensuring that team managers and their team adhere to the relevant requirements.

QFP Employees

Employees are responsible for ensuring they act in accordance with the Data Protection requirements outlined in this document and do not cause a breach of customer data as a direct result of their actions.

Member Firm Principal

It is a Member Firm Principal's responsibility to ensure their firm, advisers and employees act in accordance with Data Protection Law and are instructed in their Data Protection responsibilities.

It is also Member Firm Principal's responsibility to ensure their advisers and employees:

- Are trained and understand the principles of Data Protection, how it affects what they do and adhere to the Guidance provided to them;
- Complete any mandatory Data Protection and Information Security training;

- Have read this policy along with the Data Security Policy & Procedures; and
- Are aware of their accountability and that 'wilful' failure to comply or report a potential breach of data is potentially a disciplinary offence.

Monitoring and Risk Management

Supervisors

QFP Supervisors work 'in the field' with Member Firms to review their data management arrangements and ensure the QFP Data Privacy and Data Security procedures are implemented.

The QFP Supervisor is responsible for seeking evidence from the Member Firm to demonstrate they have adequate procedures in place and to ensure the Member Firm can be accredited as part of their on-going competency assessment program.

Risk Management Team

This team is responsible for monitoring the overall risk posed by activities of AR firms including Data Protection and security. Findings from the field-based supervision team are fed to the Risk Management team and they will use this MI to highlight potential risks through regular reporting.

Complaints Handling and Contact

Any complaints in relation to Data Protection and breaches should be referred to The Office of Data Protection or to the AR firm's DPO if appointed.

The Office of Data Protection
Quilter Financial Planning Limited
Riverside House
The Waterfront
Newcastle upon Tyne
NE15 8NY

Or via email at QFPdataguardian@quilter.com

If the data subject is not satisfied with the response, or believe QFP are not processing their personal data in accordance with the Law, they can complain to the ICO:

Information Governance Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

www.ico.org.uk/concerns