DATA PROTECTION POLICY

INTRINSIC

Policy Owner: Data Guardian

VERSION HISTORY

DOCUMENT VERSION	DATE	AUTHOR	COMMENTS
V1.0	08/12/10	Rob Rew	Issued to staff and AR Firms as part of DPA refresher training in 1st qtr. 2011
V1.1	31/08/12	Jason Rickards	Change of Data Security Officer and review of Policy. Updates to Mint name, addition of Blueprint and change from DPO to DSO for consistency
V2.0	08/01/14	Carly Robbins	Update to reflect change of DSO
V3.0	14/07/15	Dominic Newton / Parul Parmar	Update to reflect change of Data Security Officer and change from DSO to Privacy and Risk Officer & addition of Head of Risk
V4.0	16/11/17	Luke Lawton	Updated to reflect personnel changes, removed DSO and added Luke Lawton (Information Security Manager) as currently responsible for DPA.
V5.0	22/03/18	Joanne Ellerby / Julie Darlington	Updated to reflect new requirements under GDPR
V6.0	24/04/18	Joanne Ellerby	Updated scope to include definition of member firms
V6.1	25/04/18	Michelle Graham	Final reformatted version for publication
V6.2	14/05/2018	Joanne Ellerby	Amended DPP list to include DPP 5 and team manager responsibilities section

INTRODUCTION

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

As a company, IFS 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 General Data Protection Regulation (GDPR). Our policy framework sets out the necessary requirements and principles to manage and mitigate key risks and ensure compliance with the GDPR.

IFS 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 IFS's reputation. IFS 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 IFS. It sets out, and provides the high level approach to implementing and maintaining an adequate and effective data privacy risk management framework which, alongside other policies, contributes to a system of internal controls.

This policy sets out IFS's approach to how it collects, processes, manages, transfers, discloses, retains and destroys any personal data either controlled or processed by IFS, 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 IFS. In this context IFS 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 IFS.

Data Privacy controls should be proportionate to the data protection risks, relevant to IFS'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 IFS, including AR member Firms, understands their obligations to operate within the GDPR in order to:

- Assure the data privacy of customers, staff, advisers and other individuals who interact with IFS 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 IFS, Member (AR) Firms, Advisers and Employees and any 3rd party suppliers of services to IFS, 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 IFS 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 OMW Group Data Privacy Policy which is the responsibility of the Group Policy Owner ("Group Policy Owner"). The IFS Data Guardian will be appointed as the IFS Policy owner.

The IFS 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 IFS Policy Owner is expected to attest to the Group Policy Owner that their Business is in compliance with the requirements of this Policy and 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 Data Guardian who may escalate to 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 IFS Member (AR) Firms, Advisers, Clients and Employees and any contractors or 3rd party suppliers of services to IFS
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.'

GDPR PRINCIPLES AND REQUIREMENTS

The GDPR 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.

The GDPR 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, IFS 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. IFS is required to cooperate, on request, with the ICO in the performance of its tasks.

More detailed information about the GDPR can be found by reading the Information Commissioner's Office guide to GDPR found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

TERRITORIAL SCOPE

The GDPR broadly applies to all organisations in the EU, and those outside the EU that process data about individuals in the EU.

According to Article 3 (Territorial Scope) the GDPR applies to both:

a) any processing of personal data by a data controller that has its main establishment in the EU, and
b) any processing (including monitoring) of personal data of data subjects within the EU by a data controller with its main establishment outside the EU.

Further, according to Article 27, in the case of b) above, the controller shall designate in writing a representative located in the EU, to act as a contact point for regulators and data subjects with regard to the relevant processing.

In short, this means that the GDPR applies to IFS and all AR member firms.

Further detail about the responsibility of data controllers can be found in the Joint Data Controller Guidance document in the appendices.

THE PRINCIPLES

The GDPR is, like the DPA, underpinned by a number of data protection principles which drive compliance. While the data protection principles under the GDPR are similar to those found in in the DPA, certain concepts are more fully developed.

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 data subjects 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 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 the GDPR

GDPR REQUIREMENTS AND IFS GUIDANCE

The legislation itself can be complex, however, it is underpinned by the following requirements which ensure that IFS, Member (AR) Firms, Advisers and Employees meet the terms of that Regulation.

The GDPR requirements are emboldened and assigned a unique identifier, for example: **D**ata **P**rivacy **P**olicy requirement number 1 is **DPP 1**.

Underneath each of the GDPR requirements is a summary of the IFS policy and guidance response and where it can be found.

DPP1 AR firms must appoint an appropriately qualified in 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.

Individual with Data Protection Responsibilities Guidance – Appendix A

This document outlines the standards applicable to firms and to clarify the need for a 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:

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

Recording Processing Activities Guidance – Appendix B

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 set out in the GDPR. Records must be maintained of each processing activity that involves personal data, which demonstrate compliance with the following principles in each case.

- Fairness, transparency and lawfulness
- Purpose limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Confidentiality and Integrity

Lawful Basis for Processing Guidance – Appendix C

For processing to be lawful under the GDPR, 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 – Appendix D

The "Data Controller Guidance" document provides an explanation of the data controller responsibilities that are on AR firms and the relationship between IFS 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 Categories & Criminal/Civil Offence Data Guidance – Appendix E

The Special Categories and Criminal Offence Data Guidance outlines the requirements of the GDPR with respect to special category data 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 – Appendix F

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

Data Retention Schedule – Appendix G

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

Data Disposal Guidance – Appendix H

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 – Appendix I

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
- Purpose limitation – e.g. only use data for the purposes it was collected

Third Party Supplier Guidance – Appendix J

Guidance on firms interactions and agreements with 3rd parties.

DPP4 Processes and procedures must be maintained to assure data subjects' rights 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 the GDPR.

Individual Data Rights Policy – Appendix K

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
- The right not to be subject to automated decision-making including profiling

Individual Data Rights Guidance document – Appendix L

The Guidance/Process document provides the process that IFS, 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.

Automated Decision Making and Profiling Guidance – Appendix M

DPP5 Processes and procedures must be maintained to ensure any data breach 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 – Appendix N

Any incident of suspected data protection breach 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.

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 document - Appendix O

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.

Privacy Notice (AR to clients) – Appendix P

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

Internet version of Privacy Notice (AR to clients) - Appendix Q

Internet version/summary of Privacy Notice to be used by AR firms for their network 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 Data Guidance – Appendix R

Although none of the specific scenarios where GDPR 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 (DPIA) Guidance – Appendix S

Under the GDPR, IFS 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 by complying with the GDPR 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.

COOPERATING WITH SUPERVISORY AUTHORITIES

Article 31 states that the controller (IFS 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 the GDPR. Data Controllers will need to demonstrate that any processing activities undertaken comply with the GDPRs requirements and keep records of those activities to be made available to supervisory authorities on request.

Under the GDPR 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 the GDPR 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 compliance with the GDPR upon request from the supervisory authorities.

GOVERNANCE AND OVERSIGHT

Everyone in IFS, including AR member firms, has a duty to treat all personal data in accordance with the GDPR 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 IFS GDPR Data Privacy Policy and supporting guidance and procedures.

IFS EXECUTIVE

The Executive accept all reasonable obligations in respect of ensuring IFS operate in accordance with the GDPR, 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/OFFICE OF THE DPO

IFS has appointed OMW Group to fulfil its obligations to have in place a suitably qualified and experienced data protection officer. At local level IFS will have in place a Data Guardian to assist the data protection office in their role and to inform and advice 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 IFS, it is the responsibility of the Team Managers to ensure their team adhere to the GDPR and that all current and future employees are instructed in their GDPR responsibilities. This means employees:

- Understand the principles of the GDPR and how it affects what they do and have read 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 IFS Employee Handbook.

The team managers GDPR "checklist" should assist in ensuring that team managers and their team adhere to the GDPR requirements.

IFS EMPLOYEES

Employees are responsible for ensuring they act in accordance with the GDPR 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 the GDPR 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 the GDPR, 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.
- 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

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

The 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 the 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
Intrinsic Financial Services Group
Wiltshire Court
Farnsby Street
Swindon SN1 5AH

If the data subject is not satisfied with the response or believe we are not processing their personal data in accordance with the law they can complain to our regulator:

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

0303 123 1113

www.ico.org.uk/concerns