IT Security, Privacy and Data Protection Policy
Fitzgerald & Law

1. Policy Summary

1.1. The Senior Management Team within F&L ("F&L") are committed to comply with all relevant UK and EU laws in respect to data privacy and towards the protection of the "rights and freedoms" of individuals whose information F&L, as data controller, collects. Most notably in accordance with the General Data Protection Regulation (GDPR), which comes into force from the 25th May 2018. To that end, the Senior Management Team have developed and implemented and will maintain and continuously improve a documented Information Security Management System ('ISMS') within the framework of ISO 27001.

2. Scope

2.1. This policy aims to meet the requirements of the GDPR across all locations, employees, partners and affiliates of F&L who act as processor on behalf of our data subjects. Significant changes to data privacy laws in the EU/UK have led to reviewing its existing policies and procedures to ensure it meets the new criteria and to safeguard our business and clients from the latest threats towards the overall rights and freedoms of individuals.

2.2. The General Data Protection Regulation replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

2.3. The Information Security Team for F&L is responsible for the ongoing maintenance, effectiveness and ultimate alignment of this policy to fulfil legal/regulatory requirements and remains accountable on its overall performance.

3. Objectives of the ISMS

3.1. The objectives for the ISMS will enable F&L to (a) meet its own privacy requirements as a data controller; (b) to meet all necessary compliance obligations as per the GDPR; (c) impose controls in line with F&L's Risk Management strategy; (d) ensure F&L meets all applicable statutory, regulatory, contractual and professional duties and (e) that it protects the interests of data subjects, third parties, affiliated data processors and other interested parties.

3.2. F&L is committed towards the fulfilment of all its compliance requirements relating to Data Privacy and its subsequent practices including, but not limited to:

- Processing personal information only where this is strictly necessary for legitimate business purposes
- Collecting only minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by F&L, as both data controller and processor
- Maintaining its accuracy and, where necessary, kept up to date
- Retaining personal information only for as long as is necessary for both legal and/or regulatory reasons or, for other legitimate purposes – expressly agreed
- Respecting an individuals' rights in relation to their personal information, including their right to access
- Maintaining its security and accessibility
- Only transferring personal information outside the EU in circumstances where it can be adequately protected and is necessary
- The application of the various exemptions allowable by the current data protection legislation
- Developing and implementing an ISMS to enable the policy to be implemented effectively
- Where appropriate, identifying both internal and external stakeholders and the degree to which these stakeholders are involved in the governance of F&L's ISMS
- The identification of stakeholders with specific responsibility and accountability for the ISMS.

4. Notification

4.1. F&L has notified the Information Commissioner that it is a data controller and that it processes certain information about data subjects. F&L have identified personal data assets that it processes and is contained within the Data Inventory.

4.2. A copy of the ICO notification details are retained by the Data Protection Officer and the ICO Notification Handbook is used as the authoritative guidance for notification.

4.3. The ICO notification is kept updated whenever a significant change occurs.

4.4. The Information Security Team are responsible for reviewing the details of notification yearly, in the light of any changes to F&L's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments as part of their internal audit process.

4.5. The policy applies to all Employees/Staff (and its interested parties) of F&L such as outsourced suppliers. Any breach towards GDPR or the ISMS will be dealt with under F&L's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

4.6. Partners and any third parties working with or for F&L who have or may have access to personal information will be expected to have read, understood and to comply with this policy. No third party may access personal data held by F&L without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which F&L are committed and which gives F&L the right to audit compliance with the agreement if required.

5. Definitions

5.1. Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data to offer goods and services or monitor the behaviour to data subjects who are resident in the EU.

5.2. Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

5.3. Personal data – 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.

5.4. Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5.5. Data controller – the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

5.6. Data subject – any living individual who is the subject of personal data held by F&L.

5.7. Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5.8. Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

5.9. Personal data breach – a breach of security leading to the accidental or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

5.10. Data subject consent - means 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.

5.11. Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

5.12. Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

5.13. Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

6. Responsibilities

6.1. F&L is a data controller and data processor under the GDPR.

6.2. Top Management and all those in managerial or supervisory roles throughout F&L are responsible for developing and encouraging correct information handling practices, responsibilities of which are set out within staff handbooks.

6.3. The Information Security Team is accountable to Top Management directly for the management of personal information within F&L and for ensuring overall compliance with data protection legislation and best practice can be demonstrated. These accountabilities include:

- the development and implementation of the ISMS as required by this policy; and
- the security and risk management in relation to compliance with the policy.

6.4. The Information Security Team who Top Management consider to be suitably qualified and experienced, have been appointed to take overall responsibility for F&L's compliance with this policy and the day to day management on this basis and, in particular, have direct responsibility for ensuring that F&L complies with the GDPR, as do the senior management team in respect to the data processing activities that takes place within their area of responsibility.

6.5. The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

6.6. Compliance with data privacy legislation is the responsibility of all active employees of F&L who process personal information on behalf of the data controller.

6.7. Members of F&L are responsible for ensuring that any personal data supplied by them and that is about them, is accurate and up to date.

7. Risk Assessment

7.1. To ensure that F&L are aware of any risks associated with the processing of the variable types of personal information we hold and process.

7.2. F&L has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing tasks undertaken by other organisations on behalf of F&L. F&L shall manage any risks which are identified by the risk assessment to reduce the likelihood of a non- conformance with this policy.

7.3. Where a type of processing, uses new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, F&L shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

7.4. A single assessment may address a set of similar processing operations that present similar high risks.

7.5. Where, as a result of a Privacy Impact Assessment, it is clear that F&L is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not F&L may proceed must be escalated for review to the appointed Data Protection Officer who shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioners Office.

7.6. Appropriate controls will be selected, typically relating to our ISO27001 certification, and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to F&L's documented risk acceptance criteria and the requirements of the GDPR.

8. Data protection principles

8.1. All processing of personal data must be done in accordance with the following data protection principles:

- Personal data must be processed lawfully, fairly and transparently.
- Demonstrate transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language.
- The specific information that must be provided to the data subject must as a minimum include:
  - the identity and the contact details of the controller and, if any, of the controller's representative
  - the contact details of the Data Protection Officer, where applicable
  - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
  - the period for which the personal data will be stored
  - the existence of the rights to request access, rectification, erasure or to object to the processing
  - the categories of personal data concerned
  - the recipients or categories of recipients of the personal data, where applicable
  - where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
  - any further information necessary to guarantee fair processing
- Personal data can only be collected for specified, explicit and legitimate purposes.
- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of F&L's GDPR registration.
- Personal data must be adequate, relevant and limited to what is necessary for processing.
- The Data Protection Officer is ultimately responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the appointed Data Protection Officer.
- The Information Security Team will ensure that, on an annual basis all data collection methods are reviewed by internal auditors to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by F&L – as per the documented procedures, the appointed Data Protection Officer is ultimately responsible for ensuring that it is securely deleted or destroyed in line with internal policies.
- Personal data must be accurate and kept up to date.
- Data that is kept for a prolonged period of time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- The Practice Manager is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by F&L is accurate and up to date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

8.2. Clients should notify F&L of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of F&L to ensure that any notification regarding change of circumstances is noted and acted upon.

8.3. The Information Security Team is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

9. Personal Data Format

9.1. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

9.2. Where personal data is retained beyond the processing date it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

9.3. Personal data will be retained in line with the retention of records policies and, once its retention date is passed, it must be securely destroyed.

9.4. The Information Security Team must specifically approve any data retention that exceeds the retention periods defined and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

10. Data Processing

10.1. Personal data must be processed in a manner that ensures its security.

10.2. Appropriate technical measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

10.3. These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

10.4. F&L Limited's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013

10.5. Security controls will be subject to audit and review.

10.6. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

10.7. The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

11. Safeguards

11.1. An assessment of the adequacy by the data controller of its safeguards are carried out, addressing the following factors:

- the nature of the information being transferred
- the country or territory of the origin, and ultimate destination, of the information
- how the information will be used and for how long

12. Accountability

12.1. The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

12.2. Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform PIAs (Privacy Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

13. Data subjects' rights

13.1. Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.

13.2. Data subjects may make data access requests.

14. Complaints

14.1. Data Subjects who wish to complain to F&L about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer at F&L.

14.2. Data subjects may also complain directly to the Information Commissioners Office.

15. Consent

15.1. F&L understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

15.2. F&L understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

15.3. In most instances consent to process personal and sensitive data is obtained routinely by F&L using standard consent documents e.g. when a new member of staff signs a contract of employment.

16. Security of data

16.1. All Employees/Staff are responsible for ensuring that any personal data which F&L holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by F&L to receive that information and has entered into a contracted agreement.

16.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy

16.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees of F&L.

16.4. Manual records may not be left where they can be accessed by unauthorised personnel. As soon as manual records are no longer required for day-to-day client work they must be securely disposed.

16.5. Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

17. Rights of access to data

17.1. Data subjects have the right to access any personal data (i.e. data about them) which is held by F&L in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by F&L and information obtained from third party organisations about that person.

17.2. Subject Access Requests are dealt with by the Data Protection Officer and anyone nominated to act on their behalf.

18. Disclosure of data

18.1. F&L must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of F&L's business.

18.2. The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- to protect the vital interests of the individual, this refers to life and death situations

18.3. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

19. Disposal of records

19.1. Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

20. Data Protection Officer

20.1. For any/all enquiries relating to this policy or any data privacy practices carried out by F&L, please contact the appointed Data Protection Officer. All communications are to be made in writing and addressed directly to the appointed Data Protection Officer. The Data protection officer is: Alexandra Womphrey and can be contacted in writing: F&L, New Penderel House 4th Floor, 283-288 High Holborn, London WC1V 7HP.

21. EU-US Privacy Shield

F&L complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union to the United States. F&L has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program and to view our certification, please visit https://www.privacyshield.gov/

In compliance with the Privacy Shield Principles, F&L commits to resolve complaints about our collection or use of your personal information. EU individuals with enquiries or complaints regarding our Privacy Shield policy should first contact F&L's data protection officer:

Alexandra Womphrey can be contacted in writing at: F&L, New Penderel House, 4th Floor, 283-288 High Holborn, London WC1V 7HP or via email at awomphrey@fitzandlaw.com

F&L has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU.

We will never disclose your personal information to a third party except where previously agreed with you via contract. The explanation for this and the personal data transferred will be made explicit in the contract.

As above you have the right to request what personal data we hold about you and have the right to limit or withdraw consent for us to process said personal data.
F&L are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Where applicable an individual can request binding arbitration to resolve issues.

F&L may be required by law to disclose personal information in response to requests from public authorities, including to meet national security or law enforcement.

Where F&L have transferred personal data to third parties our liability will still apply.

Technical Addendum

With the introduction of GDPR as a springboard, F&L have implemented a rigorous set of software and hardware changes to ensure that the data entrusted to us is safe, secure and protected at all times.

To ensure the security of a network from the top down, F&L are using an enterprise grade network security service, which offers leading Threat Management including intrusion prevention and detection, firewall, antivirus, app control and data loss prevention, all wrapped up in a single management interface allowing us rapid response to any threats.

Internally F&L have implemented an Enterprise File Service that enables complete top to bottom control, tracking and security for all data held. Comprehensive data protection is enforced at all end points ensuring wherever we are, your data is safe and we are using the latest version. In the event of a theft of a device containing F&L data, we can remotely wipe that device to prevent any data loss. Compliance and auditing tools allow us to easily track personal data through our systems and locate all instances of an individual's data. A continuous backup is mirrored to the cloud, meaning there is no risk of data loss due to hardware errors or viruses.

Alongside new hardware and software, F&L have implemented internal policies designed to reassure you that your data is safe with us. All staff log in with Multi Factor Authentication, making the risk of an unauthorised user gaining access via a member of staff's account virtually impossible. There is also a comprehensive staff training regime, ensuring all employees are aware of information security issues and their responsibilities in ensuring your data is safe.