What is the EU General Data Protection Regulation (GDPR)?

The GDPR is a regulation designed to strengthen and unify data protection for all individuals within the European Union, aiming to give control back to citizens and residents over their personal data. The GDPR has been drawn up by the European Parliament, the Council of the European Union and the European Commission and is effective from 25th May 2018.

Taking data security and privacy seriously

At Fitzgerald & Law, we take data security and privacy extremely seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights.

Under any compliance regime, it is easy to state compliance but much harder to prove. To this end, we are implementing an information security management system which is certified to the requirements of ISO27001:2013.

By gaining certification to ISO27001:2013, Fitzgerald & Law can ensure that the appropriate controls for the management of information are in place and that we are working to meet our legal and regulatory requirements, including those outlined in the GDPR.

By working with an accredited data security consultancy, we aim to achieve ISO27001:2013 certification within the first half of 2018.

For more information about the actions we are taking please see the information below:

- Information Security Management System
- Policies & Procedures
- Frequently Asked Questions (FAQs)

Thank you for trusting us with your business and please be assured that we will always take the security and privacy of our client data very seriously.

Martin Ranson
Fitzgerald & Law LLP

Information Security Management System (ISMS)

How do you ensure that personal data is handled appropriately?

Fitzgerald & Law (F&L) operates and maintains an Information Security Management System (ISMS) to control information assets appropriately. This system was operational in 2017 and will be certified to the information security standard ISO 27001 in the first half of 2018.

We implement technical, procedural and human security controls to ensure that our information assets (including personal identifying data) are protected from unauthorised access, unwanted disclosure, modification, theft/loss, denial of service attacks or any other threat.

F&L have implemented and apply internal policies and procedures that support the ISMS. As part of the management system they will be independently audited by a certification body at least annually.

To achieve end to end security and privacy for your data, processes are designed with security best practices, privacy by design and the Plan Do Check Act (PDCA) cycle. The elements of PDCA are:

- Plan – Identify the problem, requirements, threats and control objectives.
- Do – Deploy and test solutions, processes and technologies to reduce risk and avoid operational failure.
- Check – The effectiveness of the solutions by examining the output and validating the operation.
- Act – On the results of any outputs or failures to improve effectiveness and efficiency and achieve the best solution that meets the objectives and enables business.

How do you ensure that personal data is handled appropriately?

F&L run internal audit procedures on the data we hold to ensure that we have a thorough understanding of what types of data are held as part of the business process, as well as the level of protection required for the identified data sets and what further controls we can introduce to reduce the likelihood of an incident impacting these assets in the future.

How do you manage risks and incidents relating to information assets?

F&L uses an information security risk management framework to identify, categorise and assess the likelihood of known or potential risks to the information assets within the business. The framework allows us to analyse information assets against the possible loss of confidentiality, integrity and availability which enables us to define appropriate controls in response.

A formal incident management process is used to identify, contain and recover from a security incident, should one occur, and we use this process to prevent a reoccurrence.

What training do staff go through?

As part of the onboarding process F&L provide initial security awareness training and actively promotes the key principles of information security.

Ongoing professional development takes place for all staff which includes information security updates and a compliance process to ensure all employees are up to date.

What legal, regulatory and contractual requirements do you operate under?

F&L complies with all legal, regulatory and contractual requirements related to information security and adopts UK law guidelines, industry standards and best practice for information security.

Policies & Procedures

F&L have developed policies and procedures based on industry and vendor best practices to protect the information assets it keeps for clients, partners and our own information assets. Our policy and procedures set standards for our information security controls, some examples being:

- Information Security Policy
- Clear desk and clear screen policy
- Asset management policy
- Acceptable use policy
- Mobile computing policy
- Encryption policy
- Incident management procedure
- Information classification policy
- Risk management procedure
- Disaster recovery procedure
- Internal audit procedure
- Document and record control procedure
- Corrective actions procedure
- Preventative actions procedure

Each policy and procedure support's the controls laid out by the ISO 27001 standard Statement of Applicability and how F&L manages information assets.

For further information on how we process, collect, store, share and handle your data please read our privacy policy.

Frequently Asked Questions (FAQs)

Is Fitzgerald & Law a data processor or a data controller?

For our clients, we act as a data processor meaning that we process your personal data on your behalf in accordance with the agreed contract.

Have you appointed a Data Protection Officer (DPO)?

Yes, our DPO is Alexandra Womphrey (Practice Manager).

How do you comply with the requirements of the GDPR principles?

GDPR lays out 6 principles within the framework, they are:

1. Lawfulness, fairness and transparency

We will process any personal data we collect in a fair, lawful and transparent manner and in accordance with a data subject's rights. As a client of F&L we will only process the personal data we obtain in accordance with our agreed Letter of Engagement, its defined services and terms and conditions.

2. Purpose Limitations

We will only collect personal identifying data for specified, explicit and legitimate purposes. Data we collect will not be used for any other purpose than those that the data subject has been made aware of.

3. Data minimisation

We will only collect personal data that is needed, adequate and relevant for the specific purpose.

4. Accuracy

To the best of our ability we will ensure that any personal data held is accurate, kept up to date and correct. Our systems are designed to maintain a high level of integrity meaning that any obtained data will remain as entered and unchanged.

5. Storage limitations

We will only keep personal data we obtain for as long as it is needed to comply with regulatory requirements. As a client you have the right to request erasure of individual data where doing so does not breach regulatory requirements in terms of data storage.

6. Integrity and confidentiality

All personal data collected is held in a manner that protects against unwanted modification, disclosure or unlawful processing. We take a risk-based approach to ensure that our systems have the appropriate technical and organisational controls to safeguard the integrity and confidentiality of all personal data.

Do you perform Privacy Impact Assessments (PIA)?

We perform periodic risk assessments in accordance with the ISO 27001 standard which address the confidentiality, integrity and availability requirements of any data held by F&L. Our assessment methodology includes a full assessment of what data we hold, where this information is located, the risks involved with processing this information and the controls necessary to address the associated risks.

Will I be notified in the unlikely event of a breach?

Under GDPR regulations F&L is required to report data breaches to the Information Commissioner's Office (ICO) within 72 hours. As part of our information security incident management procedure, communication includes notification to all affected parties.

How do you ensure you meet with the privacy by design requirements?

As part of our information security management system, we have implemented system development principles to ensure that whenever we develop or introduce new systems, privacy and security requirements are considered at every stage.

Where is my data stored?

Currently data is held on secure servers and backed up regularly to multiple locations. However, as part of our preparation for GDPR we are moving to a cloud-based data storage system utilising Amazon Web Services (AWS) whose servers are located in Ireland. When this is implemented, data will never be stored outside the EU.