FS SOLUTIONS
FINANCIAL SERVICES SOLUTIONS

GENERAL DATA PROTECTION REGULATION "GDPR"

The GDPR came into force as of 25th May 2018 to supersede its predecessor under the EU Data Protection Directive.

The GDPR is automatically applicable to all organisations located in the EU and to organisations located outside of the EU if they offer goods or services to EU data subjects. The new Act replaces provisions contained under the Data Protection Acts 1988 to 2003.

The GDPR emphasizes transparency, security and accountability by data controllers and processors, and standardises the right of European citizens to data privacy.

The Data Protection Commission is the national body that governs and oversees compliance with GDPR in Ireland.

Organisations involved in data processing of any sort need to be aware the regulation addresses them directly in terms of the obligations it imposes.

A fund is deemed to be a "Controller of Personal Data" under GDPR. This article examines the impact of GDPR on the funds industry.

What is personal data?

Personal data means any information related to an identified or identifiable natural person (the data subject). The data subject can be identified directly or indirectly by: name, identification number, location data, online identifiers, factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data may be held in physical or electronic format. It includes physical files, e-mails, customer relations management systems, images or recordings. The definition does not apply to deceased persons, body corporates or anonymous information (but it does apply to pseudonymised data).

What is a Data Processor?

Each service provider to a fund is considered a Data Processor under GDPR. Should a fund have appointed Data Processors, the Data Processors must provide sufficient guarantees to the fund that any processing undertaken or carried out on behalf of the fund meets the requirements of GDPR.

A data contract must be in place between the fund and each Data Processor.

What is a personal data breach?

GDPR introduced the requirement to report security breaches to the Data Protection Commissioner within 72 hours where a risk arises. In addition, funds must communicate or notify investors with undue delay of any breach to their personal data which is likely to result in a high risk to their rights to freedom, this is in addition to Central Bank of Ireland reporting.

Personal data breaches must be reported to the fund board by the Data Processor and addressed in an appropriate and timely manner.

What is a Data Subject Access Request?

Data Subject Access Requests are received from individuals (or "Data Subjects") whose personal data is held by a Data Controller. Every individual under GDPR has a right to request a Data Subject Access Request.

Data controllers must now provide the following information to the data subject, along with the actual personal data that is being sought under the access request:

1. The purposes for processing the data.

2. The categories of personal data concerned.

3. To whom the data has been or will be disclosed.

4. Whether the data has been or will be transferred outside of the EU.

5. The period for which the data will be stored, or the criteria to be used to determine retention periods.

6. The right to make a complaint to the Data Protection Commissioner.

7. The right to request rectification or deletion of the data.

8. Whether the individual has been subject to automated decision making.

The GDPR also includes the right to data portability. In particular, this new right enables an individual to require an organisation to transmit their data to another organisation.

If a Data Processor receives a Data Subject Access Request from a party, it must be reported to the fund board and addressed in an appropriate and timely manner.

What is a Personal Data Inventory?

GDPR requires a fund's Data Protection Officer to conduct an annual Personal Data Inventory, which includes confirmations from each Data Processor, on a risk-assessment basis, in respect of the data processing operations carried out on behalf of the fund.

What is a Data Privacy Impact Assessment?

Data Privacy Impact Assessments are mandatory for high risk data processing such as profiling and large scale processing of special categories of data. In the case of funds,

this would be relevant if introducing a new technology or undertaking a new project requiring the collection of data.

How can a fund board ensure compliance with GDPR?

A fund is deemed to be a Data Controller under GDPR, as outlined in the introduction, and is therefore required to implement appropriate Data Protection policies, which also require annual review by the fund board.

Accountability requires a board of directors to take a proactive and evidence-based approach to compliance with data protection rules. Since 25 May 2018, every board must be in a position to demonstrate that appropriate governance measures have been implemented to meet the standards required under GDPR.

The fund, as a Controller of Personal Data, must appoint a Data Protection Officer who monitors and oversees the appointed Data Processors. Personal Data Inventory should be reviewed annually by the Data Protection Officer and the completion of the review should be confirmed to the fund board. As part of this process, the Data Protection Officer should request confirmations from Data Processors, on a risk-assessment basis, in respect of the data processing operations carried out on behalf of the fund.

In order to monitor of oversee the fund's compliance with GDPR, the following should be reported to the fund board on a quarterly basis:

1. **Personal Data Breaches received during the period**
2. **Data Subject Access Requests received during the period**
3. **Data Privacy Impact Assessments required during the period for new processing activities**
4. **Annual Confirmations from service providers/Data Processers are on file**
5. **Fund is compliance with GDPR**
6. **Date of annual review of Data Protection Policy and status**

What amendments would have been required by GDPR to documentation?

- Investor instruction forms and prospectus or supplement documentation would have required updates to include data protection disclosures in line with GDPR

- Contracts with service providers would have required updates to comply with GDPR, particularly administrators and there would also have been a requirement for administrators to flow these terms down to sub-delegates or outsources which process personal data on their behalf, eg: transfer agency services

- The data protection policy would have required updating to align with GDPR