GDPR for Funds

Unique considerations for Investment Funds and their Service Providers.

The General Data Protection Regulation ('GDPR')

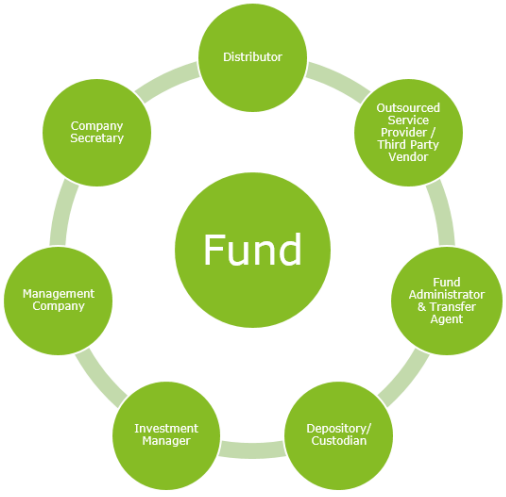
The GDPR is a regulation that comes into force on 25th May 2018 and is designed to strengthen and unify data protection for all individuals in the European Union.

It is relevant to data controllers and data processors in the public and private sector, and it applies to personal data, which is broadly speaking any information that could be used to identify a living person, regardless of whether the information is stored on a computer or held in a filing cabinet.

Investment Funds in the EU

Investment Funds ('funds') can take a number of legal and forms.

The most common forms of funds in the EU are UCITS (Undertaking for Collective Investment in Transferrable Securities) and AIFs (Alternative Investment Funds).



Funds attract a range of different types of investors from corporates, large multinationals, banks, pensions, other funds and of course individuals.

Funds generally operate under the supervision of a Board of Directors. A fund may be also be under the responsibility of a Management Company. Almost all funds will appoint a range of service providers e.g. a Fund Administrator & Transfer Agent, an Investment Manager, a Distributor, and Company Secretary. When considering the impact of GDPR on funds, each party to a fund will need to assess its own obligations.

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

Quote source
www.dataprotection.ie

Investor Personal Data

When an individual chooses to invest in a fund, they will typically be required to provide their name, address, date of birth, contact information, payment details for dividend and redemption proceeds, and tax residence information (in accordance with the US FATCA, the OECD CRS and domestic tax legislation applicable to the Fund in which they are investing).

For the purposes of identification, they may also be asked to provide photo ID and address verification along with information regarding their source of funds and wealth. They may be asked to provide additional information used to assess whether their chosen fund is suitable for them, including information about their employment, dependents, income and investment objectives.

A lot of the information provided will be necessary to fulfill the contractual requirements of the fund (as set out in its Prospectus), or to meet a regulatory requirement such as Anti-Money Laundering obligations. Nonetheless, it will be necessary for investors to provide personal data which will be processed and stored by or on behalf of the fund, and usually by one or more of the service providers to the fund.

The Transfer Agent

Personal data provided by an investor to a fund is processed in a number of ways and for a number of different purposes.

Typically, the Transfer Agent to a fund will use the information provided by an investor to update the Shareholder Register of the fund. Some of this processing may be done by the Transfer Agent in the EU, and some of the processing may be outsourced to another entity within the same group of companies, or a third party, which may or may not be based in the EU. A Transfer Agent should clearly set out what data it processes, where and how it is processed, and by which entity, when assessing its own obligations under GDPR.

A Transfer Agent should assess whether it falls within the definition of a Data Controller or Data Processor under the Regulations with regard to the data that it processes. It may be necessary to discuss this with the fund's Board or Management Company and to review the contractual arrangements between the parties as well as the direct obligations of each party imposed by the GDPR. As part of this discussion, the rationale for appointing a Data Protection Officer by one or more party to the fund should be documented, and the role and responsibilities of the DPO (especially where there is more than one) should be clearly set out.

Fundamentally, the Board of Directors of the Fund should be comfortable that there are sufficient mechanisms in place to allow for the proper governance, internal control and accountability for the personal data of the investors in the fund.

Other parties to a fund

It is fair to say that responsibility for the protection of the personal data of investors in a fund does not stop with the Transfer Agent.

The fund may also appoint a Distributor or a number of Distributors who will collect, process and store personal data.

The Investment Manager may be involved in profiling investors for the purposes of identifying new sales opportunities and market trends or to ascertain whether the fund has been sold to its intended target market.

There may be other third parties involved for the production and circulation of investor notices, financial statements and contract notes, all of which may be required

to handle the personal data of the investors in the fund.

It is worth capturing, at the outset, the role played by each party to the fund in the processing of investor personal data, in order to build a complete picture of the data flows and obligations of each party. It may be the case that certain parties are regulated (for the purposes of data protection) in their home country and not that of the domicile of the fund. It may also be the case that the processing being performed by one or more parties to the fund requires consent by the investor, and it is most likely the case that Privacy Notices will need to be updated to ensure that investors are fully aware of where their data is being processed, by whom and for what purpose.

Overall Responsibility
Without painting the full picture as outlined above, it is difficult to say where the burden of responsibility lies and where the central oversight could or should sit.

Data Controllers

"The people or bodies that collect and manage personal data are called "data controllers". They must respect EU law when handling the data entrusted to them. Data controllers determine 'the purposes and the means of the processing of personal data'.

Quote Source:
http://ec.europa.eu

Practical Next Steps
Deloitte has published a 10 Step Guide to Compliance with GDPR which sets out the practical steps that a Data Controller or Processor can take to prepare for compliance. Those 10 steps are adapted for a fund as follows, and should be coordinated centrally to capture the full impact:

Step 1 – Setting the Scene
Establish which parties are currently responsible for processing the personal data of the investors of the fund and for what purpose.

Step 2 - Contracts
Document the contractual arrangements between those parties and review the data protection provisions in those contracts to determine if they reflect the current arrangements.

Step 3 – Data Protection Officer
Determine which of the parties need to appoint a Data Protection Officer and discuss with those parties who that person is or will be and what their role and responsibilities will be in the context of the fund.

Step 4 – Data Inventory
Capture the flow of investor personal data to and between the parties to the fund, capture the legal basis for the processing and determine if investor consent is required.

Step 5 – Data Subject Rights
Review the Data Privacy Notice currently in circulation for the fund and determine if it will need to be updated and/or if investor consent is required. Establish a communication strategy for existing investors if they need to be contacted. Develop a plan for the capture and management of investor data privacy rights throughout the lifecycle of their relationship with the fund and ensure that all parties to the fund have structures in place to protect those rights.

Step 6 – Compliance Monitoring
Develop a compliance monitoring/oversight programme and set out the reporting that will be required by the Board of the fund.

Step 7 – Breach Notification
Ensure all parties have the structures in place to identify and report a breach.

Step 8 – Change Management
Discuss the change management process with each party to the fund to ensure that changes to current systems and processes incorporate 'Privacy by Design/Default'.

Step 9 – Risk Management
Review the Privacy Impact Assessment methodologies proposed by the parties to the fund in the context of each of their roles and the risks that are relevant to their business and operating models.

Step 10 - Training
Each party should develop and roll-out a Training and Awareness Programme that reflects the role that they play in processing investor data and their obligations under the GDPR.

If you are a party to a fund and would like to discuss the obligations imposed on you by the GDPR, contact us.

Contact us:

Sean Smith
Partner, Risk & Regulation
Tel: + 353 1 417 2306
Mobile: + 353 86 852 7597
Email: seansmith1@deloitte.ie

Laura Wadding
Director, Risk & Regulation
Tel: + 353 1 417 2934
Mobile: + 353 87 975 0628
Email: lwadding@deloitte.ie