WILLIAM FRY

// PRIVACY SOURCE

GDPR and the Funds Industry

The EU General Data Protection Regulation ("**GDPR**") came into effect on 25 May 2018 and has been described as the most ground-breaking piece of European Union legislation in the digital era.

The GDPR modernises the legal framework of data protection and privacy in Europe to ensure the consistent protection of personal data. The GDPR brings about a number of sweeping changes and investment funds, their administrators and other relevant delegates must review their data processes and procedures to comply with what has been the biggest change to data protection law in over 20 years.

Set out below is a summary of key GDPR-related matters that impact the funds industry.

DIRECT LIABILITY & INCREASED PENALTIES – IMMEDIATE EFFECT

Liability and penalties for breaches of the GDPR are as high as €20m or 4% of a group's annual global turnover (whichever is greater) and individuals (e.g. investors) have a right to sue for material and non-material damage arising from data protection breaches.

ACCOUNTABILITY

The accountability principle constitutes a key aspect of GDPR for the funds industry. Accountability requires a board of directors to take a proactive and evidenced-based approach to compliance with data protection rules. As of 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.

SUBSCRIPTION FORM & PROSPECTUS DISCLOSURES

Data protection disclosures in subscription forms and/or prospectus documents must be in line with GDPR, which prescribes various information to be provided to investors at the time of data collection.

CONTRACTS WITH & OVERSIGHT OF PROCESSORS

Liability principles and a requirement for more detailed terms to be incorporated in contracts with processors which necessitates updates to existing agreements between funds and various of their service providers, including, most notably, administrators. There is also a requirement for administrators to flow down these terms where they engage sub-delegates that process personal data on their behalf. With most administrators in the market continuing to operate an outsourced business model for administration services such as transfer agency, boards of directors need to examine the processes in place to ensure appropriate oversight of all delegated services which involve the handling of investor data.

GROUNDS FOR PROCESSING

The legal basis upon which data is being processed must be identified to investors at the time of data collection and, if relying on consent as a legal basis, funds should note the increased consent threshold set by GDPR, requiring consent to be documented, specific, freely-given, informed and unambiguous. It must also be easy for individuals to withdraw consent as it is for them to give it. This challenging threshold has resulted in many funds moving away from consent as the primary legal basis upon which investor data is processed.

ENHANCED RIGHTS FOR INVESTORS

New rights include the right to be forgotten, right to restriction of processing and right to data portability and these should be reflected in relevant service provider agreements, such as administration agreements as funds will require the co-operation of service providers to comply with these requests in certain circumstances. Information on how to avail of the new rights must also be provided to investors.

DPIAS (DATA PROTECTION IMPACT ASSESSMENTS)

DPIAs are mandatory for high risk data processing such as profiling and large scale processing of special categories of data. For funds, this may be of particular relevance if introducing any new technology or undertaking any new project involving the collection of investor data.

SECURITY BREACH REPORTING

The GDPR introduced a requirement to report to the Data Protection Commissioner within 72 hours where a risk arises to the rights and freedoms of individuals (such as investors). Funds must notify investors about any breaches to their personal data without undue delay where a personal data breach is likely to result in a high risk to the rights and freedoms of those investors. This is an additional obligation on top of applicable Central Bank of Ireland reporting requirements.

RECORDS MANAGEMENT

GDPR introduced an obligation to maintain detailed records of processing activities for both controllers (i.e. funds) and processors (i.e. administrators). This replaced the obligation to register with the Data Protection Commissioner.

ONE-STOP SHOP

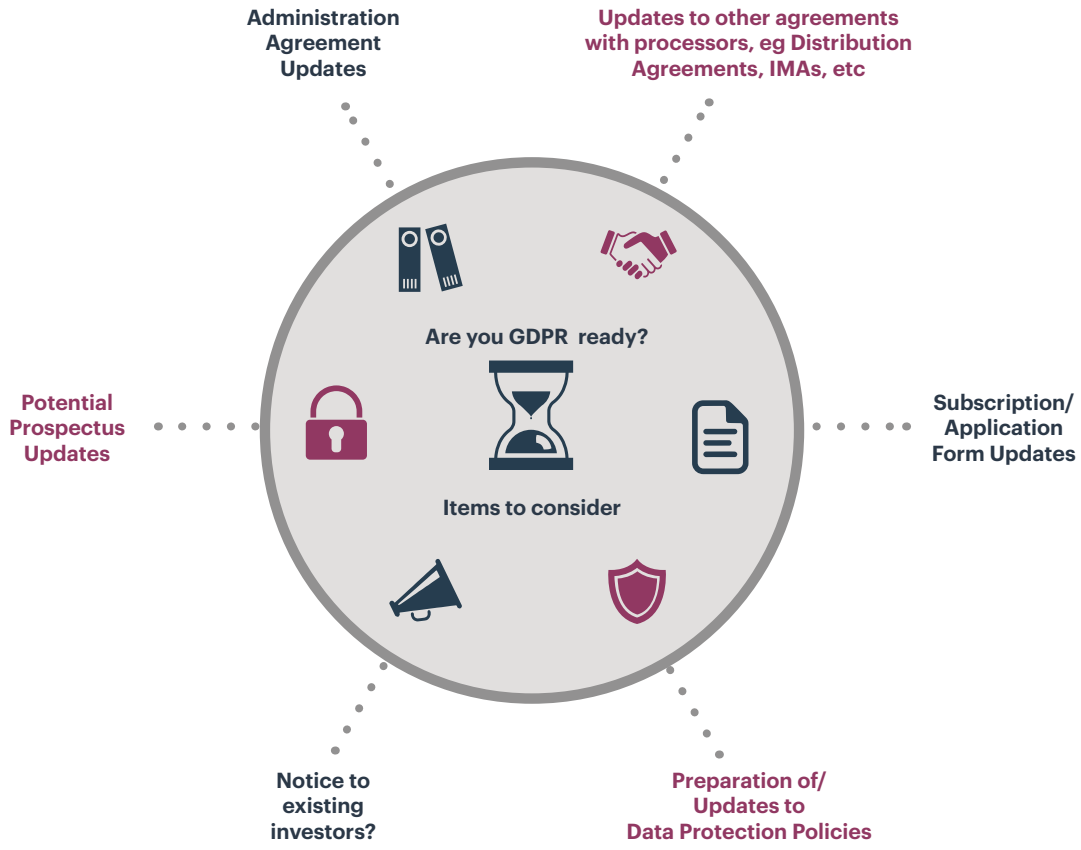
Organisations may be regulated by one supervisory authority if their main establishment is in the EU (meaning that they should only have to deal with one data protection and privacy regulator). This may, in light of Ireland's well-regarded "firm but fair" data protection regime, prove beneficial for Irish funds, e.g. in the case of claims under GDPR being taken by investors in other jurisdictions.

TERRITORIAL SCOPE

The territorial scope of data protection law was expanded under GDPR such that certain non-EU funds may fall within its scope (e.g. where they process the personal data of EU citizens such as investors based in the EU).

NEXT STEPS

Given the extensive impact of GDPR on the funds industry it is critical for all relevant stakeholders to make every effort to be compliant. Please contact any of our team for assistance with GDPR matters.



Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partners below, our your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 5183
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA