GDPR checklist for Fund Boards

The EU General Data Protection Regime (**GDPR**) was adopted last year, and comes into force on 25 May 2018. The reason for the lead in time is that it introduces a sweeping new data protection regime, and it will take some time for organisations to update their data protection policies, notices and procedures to comply with the new rules.

The GDPR will apply to all organisations established in the EU that handle personal data relating to individuals, and to those outside the EU who offer goods and services to, or monitor the behaviour of, EU residents. It repeals and replaces current EU and national data protections laws, introducing a harmonised data protection law across the EU subject to any national derogations.The Irish Government is currently drafting a Data Protection Bill which will come into force alongside the GDPR and provide for derogations, where permitted.

Irish Funds need to ensure that they are in full compliance with the GDPR (and be able to demonstrate how they comply with their data protection responsibilities) by 25 May 2018. Irish Funds are in scope where they control and are responsible for the keeping and use of personal information on computer or in structured manual files, for example, where they obtain and process customer due diligence documentation for AML/ CTF purposes. They will therefore be subject to specific statutory obligations under the GDPR, and liable to hefty fines of up to €20 million or 4% of annual turnover, as well as compensation claims from individuals for pecuniary or non-pecuniary loss (such as emotional distress) resulting from any infringement of the GDPR.

Key Obligations

The GDPR imposes more onerous data protection obligations on organisations and strengthens individuals' control over their data. Five key obligations imposed by the GDPR are detailed below.

(i) Accountability

The GDPR introduces a new concept of '*accountability*', which requires Funds to be able to demonstrate how they comply with their data protection responsibilities. Key actions which Funds are required to take under the GDPR, and which will also help demonstrate compliance, include: adopting '*a privacy by design*' (e.g. pseudonymisation and encryption) and a *'privacy by default'* (e.g. data minimisation) approach to ensure data protection is considered at the outset of a new project rather than an afterthought; conducting Privacy Impact Assessments where a Fund's processing activities are likely to result in a high risk to individuals' rights, and keeping records of processing activities.

(ii) Data Protection Officers

The GDPR requires certain organisations to appoint a Data Protection Officer (**DPO**), including organisations whose core activities involve regular and systematic monitoring of data subjects on a large scale. For example, profiling and scoring for purposes of risk assessment, including fraud prevention; detection of money-laundering or credit scoring will be deemed to be 'regular and systematic monitoring'. Whether or not such processing occurs on a 'large scale' will depend on a number of factors, including the number of data subjects and the volume of data.

The GDPR imposes mandatory obligations on DPOs, and requires their contact details to be communicated to the Office of the Data Protection Commissioner (**ODPC**).This requirement, along with the obligation to keep records of data processing activities, replaces the current requirement for organisations to register with the ODPC. If a Fund decides that it is not required to appoint a DPO, it would be prudent to document the internal analysis carried out to determine whether or not a DPO should be appointed. This analysis is part of the documentation that should be kept to demonstrate compliance with the GDPR and may be requested by the ODPC.

(iii) Privacy Notices

Funds will be required to provide a whole myriad of additional information to individuals at the time their data is collected, to ensure their data processing activities are transparent. Existing privacy policies and notices, in documentation such as Prospectus' and subscription forms, will therefore have to be reviewed and revised to meet the increased information rights of individuals. For example, individuals will have to be informed of the legal basis for processing their data; the period for which their data will be retained; details of any data transfers out of the EEA; and the existence of any automated processing, including profiling, and the consequences of such processing.

(iv) Mandatory Data Breach Reporting

All Funds will have a mandatory obligation to report security breaches to the ODPC within 72 hours of becoming aware of a breach, unless there is unlikely to be a risk to the rights of individuals. Individuals must also be informed of the breach, if there is a high risk to their rights. It will therefore be necessary to review your data breach response plans to ensure that breaches can be speedily reported.

(v) Reformed Relationship with third party service providers

The GDPR increases the contractual and statutory obligations of processors (i.e. third parties who process data on a Fund's behalf) with the result that they will be subject to fines by the ODPC and compensation claims from individuals. The GDPR contains a list of specific contractual obligations of processors which must be included in data processing contracts. It will therefore be necessary for Funds to review and revise their data processing contracts, prior to 25 May 2018, to ensure they clearly set out responsibilities and liabilities of both parties.

Stronger individuals' rights

The GDPR strengthens individuals' rights in relation to their personal data. Individuals have a new right to data portability; broader rights to request erasure; object to or restrict the processing their data; a right of access to their data; a right to rectification of inaccurate or incomplete data; and a right not to be subject to automated decision-making (including profiling) which produces a legal or other significant effect on them. These rights are not absolute and it is important to understand when they arise. For example, an individual's right not to be subject to automated decision-making, including profiling, does not apply if the decision is necessary for the performance of a contract; authorised by EU or Member State law (e.g. AML or tax laws); or if based on the explicit consent of the data subject. Funds will need to ensure they have procedures in place for dealing with individuals' requests.

Sanctions

The GDPR gives the ODPC the power to impose hefty fines on Funds of up to €20m or 4% of the total annual worldwide turnover of the preceding financial year, whichever is greater, for non-compliance with the new rules. This is a significant departure

from the current regime, where only the courts have the power to impose fines for data breaches, and such fines have remained low and few. The ODPC has, to date, adopted an "engaged" approach to regulation, striving to resolve complaints amicably, and prosecutions, for the most part, occur after an organisation has failed to heed a warning by the ODPC.

The GDPR does not grant organisations any amnesty to ease into the new rules post-25 May 2018. Whilst the GDPR sets out the criteria which supervisory authorities must have regard to when determining the quantum of the fine to impose, including, the nature, gravity and duration of the breach; the level of damage suffered; the level of co-operation between the ODPC and the regulated entity; and any previous contraventions, it does not contain an amnesty period of any description.

Liability

Individuals will have the right to bring compensation claims for pecuniary or non-pecuniary loss (i.e. emotional distress) caused by a data breach. This is a significant change in the legal landscape, as the Irish courts have, to date, refused compensation for non-pecuniary loss resulting from a data breach.

'To Do' List

It is vital that the Funds sector start taking steps now to prepare for the new rules. The following points of action provide a checklist of steps that a Fund can take.

1. Take an inventory of the personal data which the Fund holds, the purpose of collecting and processing it and to whom it is disclosed.
2. Review how the Fund is currently capturing investors' consent to the processing of their personal data, and consider whether this meets the more onerous requirements of the GDPR.
3. Review existing security policies/procedures, and implement a "privacy by design" approach to data protection (such as pseudonymising and encrypting data), and a privacy by default approach (such as only keeping the minimum amount of necessary data).
4. Review Fund data breach response plan/ procedures to ensure it can report a breach to the Data Protection Authority within the statutory 72 hour time-limit.
5. Review and update Fund prospectus and subscription documentation to meet the increased information right of individuals.
6. Review and update current agreements with third party service providers (such as Administration Agreements) to include the more prescriptive obligations of service providers which the GDPR requires to be included in data processing contracts, as well as appropriate liability apportionment clauses.
7. Carry out a Privacy Impact Assessment for any processing that may pose a high risk for data subjects' privacy rights.
8. Review arrangements to ensure that the Fund and/or any of its delegates does not transfer personal data to a country outside of the EEA unless that country ensures an adequate level of data protection or appropriate safeguards are in place.
9. Assess and understand the new and enhanced rights of individuals and obligations on the Fund and its delegates. Assess the Fund's capacity to respond to an individual's request to access, erase, rectify, port, restrict or object to the processing of their data, within the one month statutory time-limit.

It will be important for Funds to factor in the time required to gather the necessary information and to agree new processes and provisions (particularly with service providers) as well as allowing time for clearing documentation with the Central Bank, where appropriate.

Contact us if you would like a copy of our Business Guide to the GDPR.

KEY CONTACTS

Brian McDermott
Partner, Head of Asset Management & Investment Funds
+353 1 649 2307
bmcdermott@algoodbody.com

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

Michael Barr
Partner
+353 1 649 2327
mbarr@algoodbody.com

Mary McKenna
Partner
+353 1 649 2344
mmckenna@algoodbody.com

Niamh Ryan
Partner
+44 20 73 820 820
nryan@algoodbody.com

Elaine Keane
Partner
+353 1 649 2544
elkeane@algoodbody.com

Stephen Carson
Partner
+353 1 649 2317
scarson@algoodbody.com

Nollaig Greene
Knowledge Lawyer
+353 1 649 2359
ngreene@algoodbody.com

Davinia Brennan
Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com