GDPR in Context: Impacts on the Asset Management Industry

Background

The General Data Protection GDPR (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Investment fund companies, ICAVs, management companies, alternative investment fund managers ("**AIFMs**"), distributors, fund administrators and depositaries will each need to consider the extent to which they control and / or process personal data, whether relating to investors (and whether individuals, or individual business contacts for corporate, nominee or service provider entities), or their respective officers and employees, and to ensure that in each case they can demonstrate compliance with the relevant requirements of GDPR.

Scope of application

Unlike current data protection rules, which focus on data controllers which are established in the EU, the GDPR applies not only to organisations established in the EU, but also to non-EU controllers and processors where their processing activities relate to offering goods and services to individuals in the EU, or monitoring the behaviour of individuals insofar as the behaviour takes place in the EU. Non-EU investment managers and AIFMs, to the extent that they control or process personal data of EU employees or investors for such purposes, may therefore be within scope of the GDPR. Such organisations will therefore need to consider whether they are within scope and if so, whether they will need to appoint a representative in the EU for GDPR purposes.

One stop shop

The GDPR introduces the concept of a "*one stop shop*" for supervision (subject to co-operation between data protection authorities), which will require multinational organisations in particular to establish which EU supervisory authority should be their lead authority.

Controllers versus processors

As is currently the case, identification of the controller of personal data (ie the entity which determines the purposes and means of the processing) will ultimately be a question of fact, with the possibility that two or more entities might be joint controllers of the data, or separate controllers (for different purposes) of the same, or subsets of the, data.

In the context of the funds industry, investment fund companies, ICAVs, and management companies to unit trusts and common contractual funds, will be considered to be data controllers of investor data. Whether a service provider to a fund or management company is likely to be considered to be a controller or processor (or both) may turn on whether there is a direct relationship between the service provider and the individual (eg there may be a separate, direct relationship between an investment manager and an investor), and the nature and terms of the services contract in place with the fund or management company.

Where a service provider is acting on instructions from the fund or management company, as typified in the terms of an administration agreement, the service provider is likely to be considered to be a processor. It should be borne in mind, however, that the terms of a contract taken in isolation will not be determinative of the issue, and that consideration will be given to the substantive position with regard to decision-making about processing activities.

Processors should therefore not process outside the scope of the relevant contract to avoid a risk of being deemed a controller. Ambiguities have arisen on occasion, eg in the context of anti-money laundering, where a service provider may seek to review investor AML documents for the purposes of its own compliance requirements (notwithstanding that the AML obligations may be strictly those of the fund) and in the context of breach notifications, where a service provider notifies data subjects or the data protection authorities without seeking the direction of the controller.

Critically, the GDPR specifies that where a processor infringes the GDPR by determining the purposes and means of processing, it will be treated as a data controller in respect of that processing. Having established that a particular entity within a funds' universe is a processer rather than a controller, it will be important for that entity to have a clear definition of its remit with regard to the processing of the personal data in question, and to remain with the parameters of the agreed scope. The increased requirements relating to processing contracts may prove of assistance in that regard.

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Impacts on the Asset Management Industry

Privacy by design and by default

The GDPR puts personal data protection front and centre as a fundamental right of the individual, and introduces the concept of data privacy "by design and by default", which is in effect a recasting of the data protection principles and security obligations under the current EU Data Protection Directive (which has been implemented into Irish law through the Data Protection Acts 1988 and 2003 (the "**DPA**")).

The design element of the GDPR requires controllers, having regard to the state of the art and cost, to implement appropriate technical and organisation measures and procedures ensuring compliance with the GDPR. Controllers will also be expected to implement mechanisms which, by default, ensure that data can only be processed in accordance with rules which reflect the data protection principles in the GDPR.

Allied to the 'by design and by default' theme, is an emphasis on transparency and accountability as fundamental GDPR concepts, necessitating that compliance with the relevant requirements be demonstrable. Accordingly, the GDPR imposes new requirements relating to the analysis and documenting of data processing activities as part of efforts to ensure both controllers and processors are accountable for, and can demonstrate compliance with, their respective obligations under the GDPR.

Controllers

The GDPR does not, for the most part, impose wholly new compliance principles on controllers. Rather, it aims to strengthen the existing framework, by clarifying existing concepts and principles, and focusing on individual rights.

Among the key controller obligations which funds, management companies and other controllers of employee, business contact and investor data need to consider are:

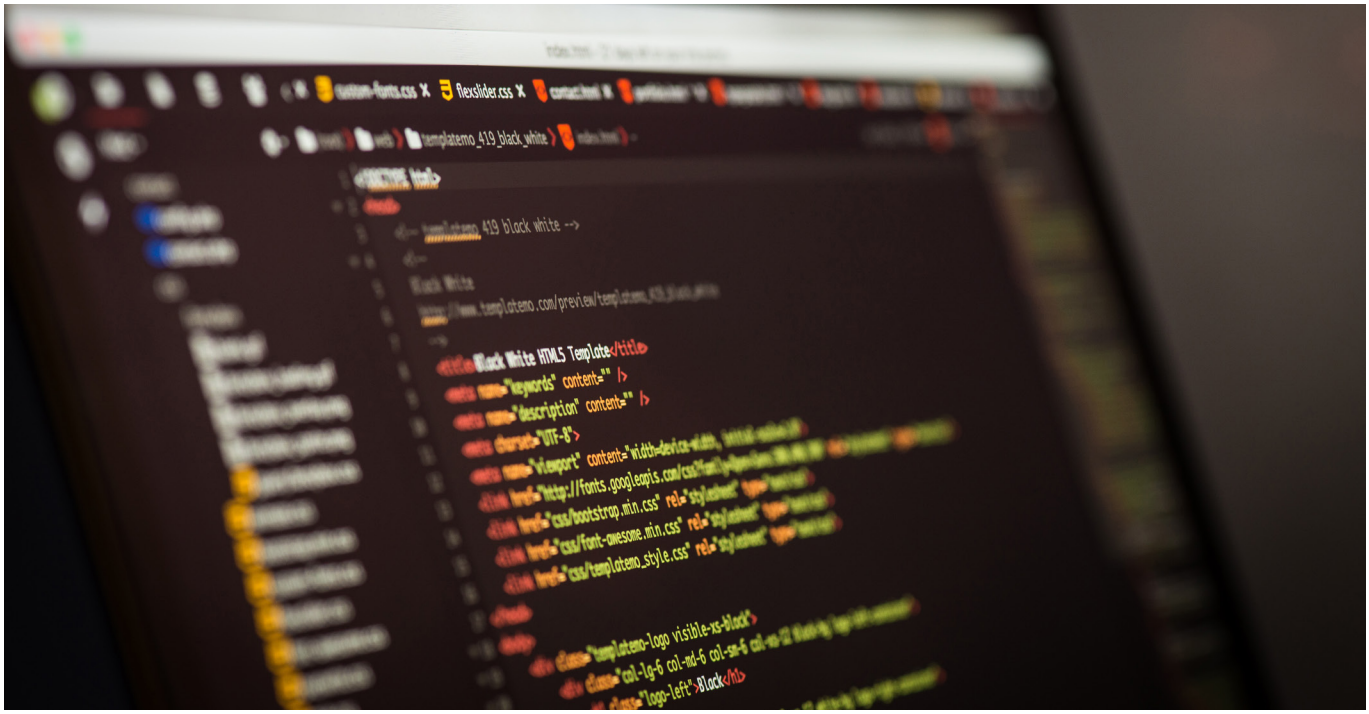
- the more explicit obligations on controllers to **communicate** with data subjects regarding the processing of their personal data, and their rights in relation to that processing, **in a transparent manner**, in concise, intelligible and easily accessible, clear and plain language.

  This will require comprehensive review of subscription and application forms, prospectus disclosures and any relevant website terms and conditions, as well as a consideration of any other methods through which personal data is collected;

- the additional and specific requirements relating to the manner in which **consent** is collected from a data subject, such that consent must be obtained on a purpose by purpose basis, using clear and plain language, in circumstances where, in order to be valid, the consent must be an **unambiguous** indication of the individual's wishes, by a statement or clear and affirmative action, and individuals must be informed that they **may withdraw** their consent at any time.

  Accordingly, the circumstances in which consent may be relied upon to legitimise processing will be narrower, and where consent is to be relied upon, there will be an impact on how this is communicated to individuals through subscription forms, the fund prospectus, etc;

- where a **legitimate purpose** of the controller is relied upon as a legitimate processing ground, the requirement that the individual be told of the justification for the processing and of his or her additional **rights to object** to or restrict processing and to have data erased;



Impacts on the Asset Management Industry

Matheson

- the continuing obligations to implement appropriate technical and organizational measures, which may include pseudonymisation and encryption, to ensure a level of **security** appropriate to the risk to the rights and freedoms of individuals associated with the processing activities, the controller having undertaken a risk assessment as the varying likelihood and severity of the risks which considers the state of the art, the costs of implementation of the measures, and the nature, scope, context and purposes of the processing;

- increased focus on the responsibility of controllers in **choosing processors** which provide sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the GDPR requirements are met and the rights of data subjects are protected, and in ensuring ongoing compliance by those processors;

- the additional requirements in relation to **processing contracts**, which will necessitate a review of all processing arrangements (including, in particular, administration agreements) currently in place, to ensure all newly mandated provisions, including those identified below, are incorporated;

- the additional and / or expanded **data subject rights** under GDPR, including rights to object, to restrict processing, data portability and the "*right to be forgotten*", as well as shorter timeframes for compliance with data subject access requests;

- **mandatory data breach notifications** to the supervisory authority, within 72 hours, unless the breach is unlikely to result in risk to the rights of individuals, and to individuals without undue delay, where the breach is likely to result in a high risk; and

- the requirement, in most circumstances, to maintain more **extensive records** of processing activities, including the purposes of the processing, the categories of data subject, personal data, recipients (including in third countries), any transfers of personal data abroad, including documentation of suitable safeguards, timelines for erasure of data, and where possible, a general description of the technical and organisational security measures applied to the processing activities. To comply with the record-keeping requirements, controllers will need to create and maintain a data register that details all data processing activities carried out by, or on behalf of, the controller.

  From the perspective of funds and management companies in particular, this will require greater transparency with regard to the processing activities of service providers, which should, however, assist in complying with the processing contract obligations outlined below, and in particular, those requiring documentation of instructions with regard to processing, and a clear description of various aspects of the processing and the obligations and rights of the controller.

  In appropriate circumstances, funds, management companies and other controllers of employee, business contact and investor data may be required to:

- undertake pre-processing data protection or privacy impact assessments ("**PIAs**"), which are required if the processing is likely to result in a high risk to an individual's rights, and which may require pre-processing consultation with the relevant supervisory authority. Such high risk processing includes profiling, large scale processing of sensitive categories of personal data, and may arise where there is innovative use of technological solutions.

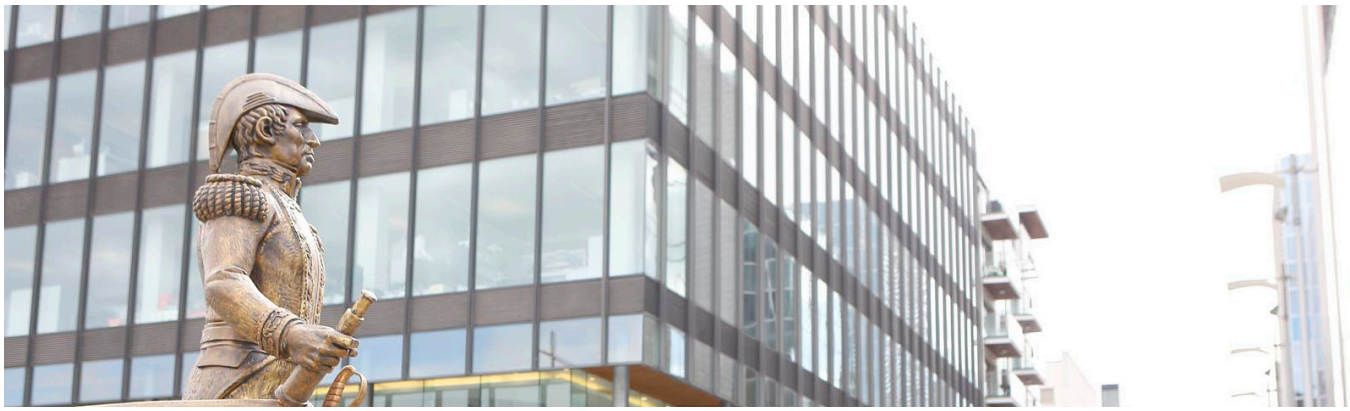
  In addition, transfers of personal data outside the European Economic Area ("**EEA**"), while not specified in the GDPR as high risk per se, have been identified by the Article 29 Working Party as amongst the factors which may be indicative of high risk. Whether a PIA may be required will therefore be a relevant consideration in the context of any offshore outsourcings by service providers; and

- appoint a data protection officer ("**DPO**"), which will be required, inter alia, where the processing:

  (i) requires regular and systematic monitoring of data subjects on a large scale; or

  (ii) involves processing large amounts of sensitive data or personal data relating to criminal convictions and offences.

  Organisations are free to appoint DPOs even if not required to do so under the GDPR, but if they chose to do so, all DPO related provisions in the GDPR will apply.



Impacts on the Asset Management Industry

Matheson

Processors

The GDPR introduces additional statutory compliance obligations directly on processors by expanding on their current obligations. It provides that a processor will be directly liable to data subjects where it does not comply with its obligations or acts outside instructions of the controller, and may be subject to direct enforcement by supervisory authorities, fines for non-compliance, and compensation claims by data subjects for any damage caused by breaching the GDPR.

Among the key processor obligations and impacts which fund service providers and other processors need to consider are:

- the continuing obligation to process only on the documented **instructions** of the controller, but combined with the express statement under the GDPR that a processor which does not comply with the instructions of its controller, and independently makes determinations about the means and purposes of the processing, will be considered to be a controller in respect of that processing activity;
- the additional **contractual undertakings** to which processors must agree, as outlined below;
- the prohibition on the appointment of **sub-processors** absent specific or general written authorisation from the controller, and the requirement that any sub-processing agreements contain the same data protection obligations that are imposed on the lead processor by the controller.

  In addition to the above, fund administrators who act as processors must consider the outsourcing provisions contained in the Central Bank (Supervision and Enforcement) Act 2013 (Section 48 (1)) (Investment Firms) Regulations 2017 (the "**2017 Regulations**"). The 2017 Regulations provide that any fund administration outsourcing arrangement must be based on a legally binding contract or service level agreement, which must contain certain mandatory provisions, including that the activities being outsourced are clearly defined and that the respective rights and obligations of the fund administrator and the outsourcing service providers are specified.

  Under both the GDPR and the 2017 Regulations, the requisite provisions are required to be reflected in the contracts throughout any chain outsourcings;
- the obligation, in most circumstances, to maintain **records** of all categories of processing activities which must contain details of the name and contact details of the processor, controller by controller details and the categories of processing, any transfers of personal data abroad, including documentation of suitable safeguards, and where possible, a general description of the technical and organisational security measures applied to the processing activities;
- the obligation to **cooperate** with the supervisory authorities;
- the obligation to notify controllers of a **data breach** without "*undue delay*" after becoming aware of it;
- the clear application of the **prohibition on transfers** outside the EEA to processors, combined with a clear statement that only the European Commission may determine whether a third country or international organisation ensures an adequate standard of data protection.
- Organisations will still be able to rely on model clauses as a valid means of transfer and the GDPR provides a list of other valid transfer mechanisms, including the potential for approved codes of conduct and certification mechanisms, provided there are binding and enforceable commitments of the controller or processor in the third country. Helpfully, the GDPR also mentions the possibility of model clauses between data processors, which do not exist at present. The GDPR also specifically sets out clear provisions on requirements and procedures in relation to Binding Corporate Rules ("**BCRs**") for the first time, which may simplify the current lengthy approval process with data protection authorities; and
- the potential requirement to appoint a **DPO** (discussed above in relation to controllers).

Impacts on the Asset Management Industry

Data processing agreements

As is currently the case, there is an express requirement under the GDPR that a written agreement be put in place between a controller and processor. This does not have to be a separate and specific processing agreement dealing exclusively with data processing activities, and the requisite provisions are generally embedded into the relevant services contract (eg the administration agreement). However, the GDPR significantly expands the mandatory content of processing agreements, to include:

- a description of the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller;
- contractual provisions obliging the processor to:
- not process other than on documented instructions, including with regard to transfers to a third country, or where required to do so by EU or EU member state law, to inform the controller in advance (unless prohibited);
- ensure that persons authorised to process have committed, or are subject under statute, to confidentiality obligations;
- comply with appropriate technical and organisational security measures, which may include encryption, pseudonymisation or other technical
- comply with the sub-processing restrictions;
- assist the controller, by appropriate technical and organisational measures, insofar as possible, to comply with the controller's obligations with regard to data subject rights;
- assist the controller in complying with its obligations relating to security, notification of breaches, and PIAs;
- at the controller's request, return or delete personal data when the agreement terminates; and
- provide the controller with all information necessary to demonstrate compliance with the processor related obligations in the GDPR and allow for and contribute to audits and inspections by the controller or its mandated auditor.

While administration agreements have tended, in more recent years, to include a broader range of processing obligations that those currently mandated under the DPA, including in relation to breach notification assistance, it is unlikely that all current services provider agreements will include all of the above requirements, and both controllers and processors will need to review and revise all relevant service provider agreements between now and 25 May 2018.

Impacts on the Asset Management Industry

Liability

The GDPR takes a multi-layered approach to remedies and sanctions for breach of its provisions. At a high level, data controllers are liable for damage caused by processing which infringes the GDPR. Data processors, on the other hand, are liable only where they have not complied with obligations specifically directed at them under the GDPR, or have acted outside or contrary to lawful instructions from the data controller. While in general, data processors have fewer obligations under the GDPR than data controllers (although more than currently apply to data processors), they may fall foul of the provisions deeming them to be controllers where they act outside their instructions.

Data controllers and data processors may only escape liability where they prove they are not "*in any way*" responsible for the event giving rise to the damage. This is combined with a "*joint and several*" style provision, which holds each involved data controller and data processor liable for the entire damage caused by the processing, in order to ensure effective compensation of the data subject, although any controller or processor which has paid the full amount of compensation is then entitled to claim back from the others involved for their corresponding part in the damage.

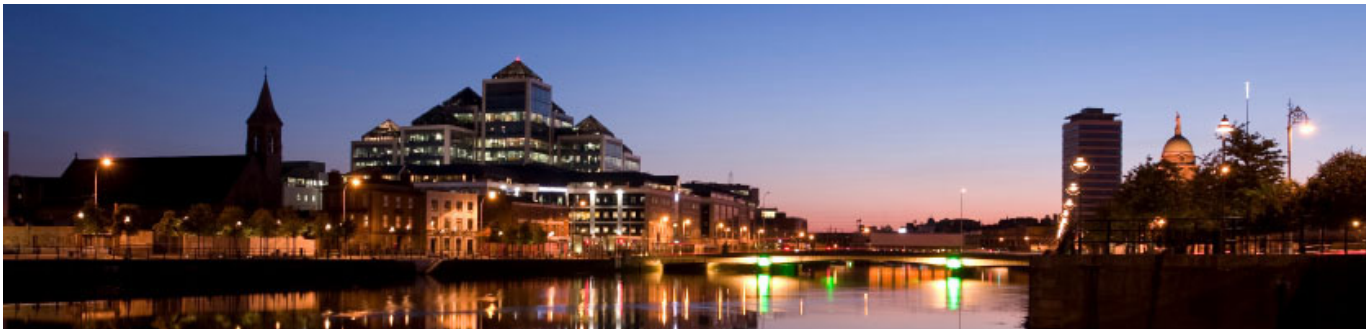
Separately, there is an administrative fines regime outlined in the GDPR, which is intended to impose sanctions that are effective, proportionate and dissuasive. The level of potential sanction will depend on the breach, and will range from fines of up to €10 million or 2% of total worldwide annual turnover in the previous financial year (for breach of principles such as "*by design and by default*", non-compliance with the processing related obligations, or failure to appoint a Data Protection Officer) to fines of up to €20 million or 4% of total worldwide annual turnover in the previous financial year (for breaches including breaches of the principles relating to processing or of the lawful processing requirements, and for breach of data subject rights).

The administrative sanction regime does not impose liability on a strict liability basis, but will require a case by case assessment of the circumstances of each individual infringement, taking into account factors such as the nature, gravity and duration of the infringement, the intentional or negligent nature of same, any damage mitigation steps which have been implemented, the technical and organisational (ie security) measures which had been implemented, and how the supervisory authority became aware of the issue.

Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning investor and other personal data which it controls or processes, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place to ensure the fundamental rights and freedoms of persons when processing their personal data.

The starting point for any GDPR compliance project is therefore an understanding of the "*what, why, how and where*" of current personal data processing by each organisation. At a minimum, for funds and their various service providers, this will require a review in advance of 25 May 2018 of all subscription agreements, prospectus disclosures, website terms, and service provider and data transfer agreements, to enable both controllers and processors within each fund's universe to demonstrate compliance with their respective obligations under GDPR.



Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.10.17