Building a better working world

What the GDPR means for the asset management industry

Minds made for protecting financial services

From tactical compliance to a principled approach to data privacy and protection: GDPR 2.0

Introduction

A broad range of companies are affected by the General Data Protection Regulation (GDPR), which came into force in each of the European Union Member States on 25 May 2018. After all, any organisation which collects and processes the personal data of EU residents will need to comply with the new regulation. While the impact of GDPR is most obvious on companies that hold and process consumer data, asset managers cannot afford to be complacent – not when the fines for noncompliance can amount to up to €20 million or 4% of global revenue, whichever is higher.

When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus — to build a better financial services industry, not just for now, but for the future.

We train and nurture our inclusive teams to develop minds that can transform, shape and innovate financial services. Our professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It's these better questions that lead to better answers, benefiting our clients, their clients and the wider community. **Our minds are made for protecting financial services.** It's how we play our part in building a better working world.

ey.com/FSminds

GDPR – what does business as usual look like?

Having worked feverishly toward day-one compliance, asset managers are also keenly aware that GDPR requires an ongoing strategic data protection effort. Here, we outline some of the ways in which the GDPR specifically affects the asset management industry, and how asset managers can embrace a sustainable and strategic data privacy approach through an intelligent data privacy framework.

Once the initial implementation deadline for the GDPR passed – and asset managers achieved all the requirements for compliance – many larger firms started thinking about GDPR 2.0. Now that the initial rush to achieve day-one GDPR compliance is in the past, what does the business as usual (BAU) operating model look like for asset managers? To answer this question, we first need to have a complete picture of how the GDPR impacts a typical asset management organisation.

GDPR – what has asset management data got to do with it?

The type of data being processed varies widely depending on the type of asset management organisation:

- **Asset managers** typically have personal data relating to any "direct to customer" retail products, as well as alternatives products (particularly real estate). Asset managers whose customer base is institutional or corporate only are less exposed to the effects of GDPR.
- **Outsourced asset servicers** process some personal data on behalf of asset managers and wealth managers. Therefore, depending on the nature of the outsource arrangement, they also process significant amounts of personal data.
- **Wealth managers and private banks** have a lot of sensitive personal data relating to high-net-worth and ultra-high-net-worth individuals.

Compliance complications caused by the complex asset management ecosystem

At the outset, asset management companies need to reconsider the extent to which they control or process personal data.

As the management of financial instruments involves a complex value chain, each party in the value chain needs to be carefully considered — from fund boards, administrators and transfer agents to investment managers, independent financial advisors (IFAS), and other retail and wholesale distributors. Each of these is typically a separate entity, with data being passed between them on a constant basis. Key data processing activities typically occur in the investment manager, the fund administrator and the transfer agent. In addition, the distribution network itself can be a complex web of intermediaries (brokers, IFAs, etc.), who are all holding personal data relating to customers and potential customers for marketing purposes.

Asset managers need to plan to address the data privacy implications of the entire value chain in order to be fully GDPR-compliant, in practice and in spirit. Naturally, this composite nature compounds the compliance complexity and necessitates a structured approach which takes this interconnectedness into account.

Asset managers also need to determine the role played by each party to fund in the processing of investor personal data, in order to build a complete picture of the data flows and obligations of each party. For example, some entities are regulated in their home country for the purpose of data protection and not that of the domicile of the fund. Furthermore, as data processing by one or more parties to the fund requires a legitimate legal basis, privacy notices will need to be updated to ensure that clients and investors know where their data is being processed, by whom, and for what purpose.

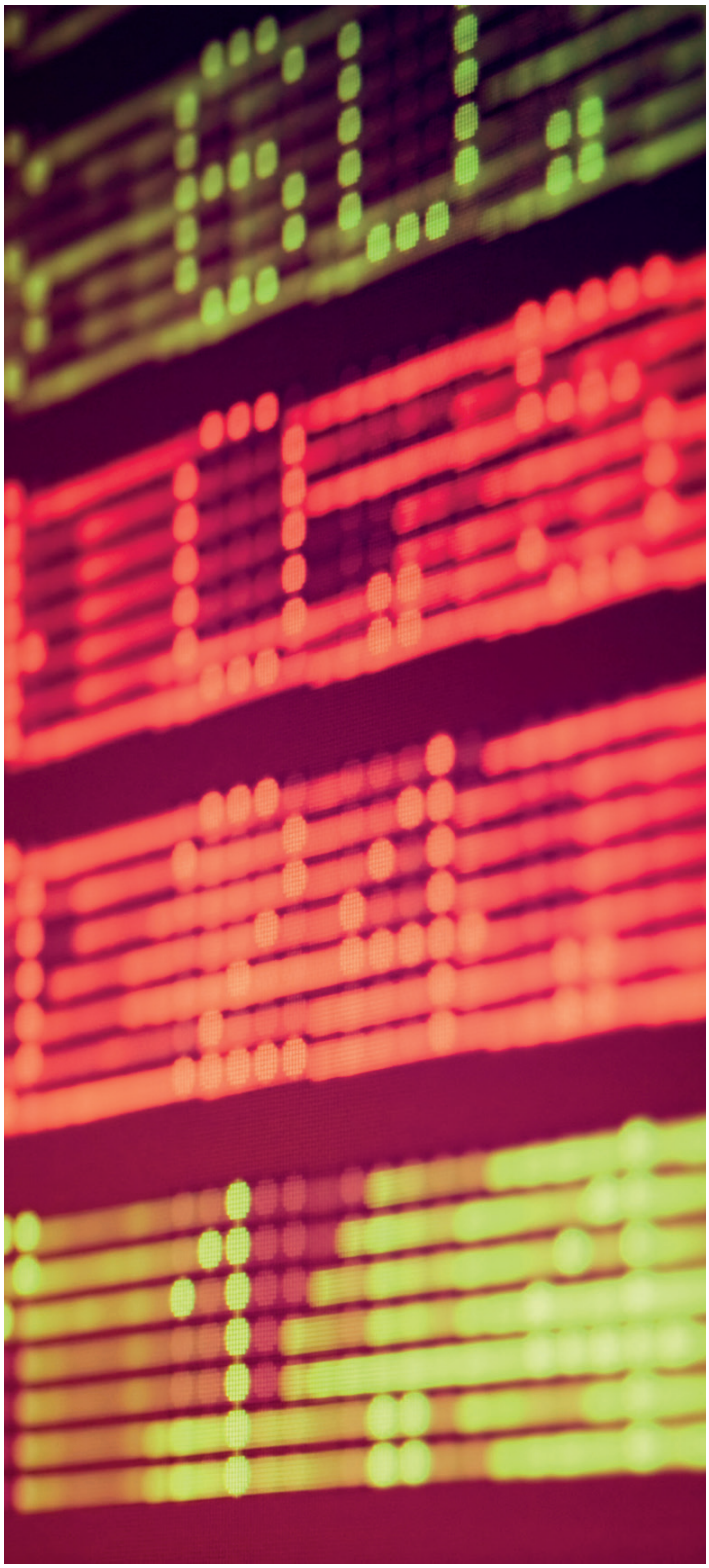
In addition, if any personal data is transferred outside of the EU (including to the EU entity's parent or sister companies), then a mechanism to transfer that personal data needs to be put in place, such as a data transfer agreement based on the model clauses or binding corporate rules (unless that country, territory or sector ensures an adequate level of protection in relation to the processing of personal data).

GDPR — privacy, but by which design?

A key tenet of GDPR is the concept of "privacy by design". What does that mean in practice?

The principle behind privacy by design is to promote privacy and data protection compliance proactively from the start. As such, this approach is the opposite of a tactical line of action that considers data privacy and protection as an afterthought or relies on a makeshift set of solutions.

EY's five-phased GDPR compliance framework is a tried and tested, industry-specific approach that takes into account the intricacies of the asset management industry, and builds on the lessons learned by our dedicated team of GDPR compliance and business consultants.



Summary-impact of the GDPR on asset managers

- Expanded notices about how personal information is to be used
- Limitations on retention of personal data
- Increased requirements to delete or hand over an individual's information upon request
- Mandatory data breach notification requirements
- Requirements to maintain records of data processing activities and transfers of personal data
- Higher standards for data controllers to demonstrate that they have obtained valid consent for certain data processing activities

A GDPR dictionary for asset managers

1

Data subject

An individual whose information is being processed

2

Data controller

An organisation or an individual who is in charge of deciding how data on the data subjects is processed and why

3

Data processor

An organisation or an individual that processes the actual personal data

4

Supervisory authority

A supervisory entity chartered to enforce privacy or data protection laws and regulations

Data subject

Asset managers are likely to control and process personal data (as defined by GDPR) relating to:

- Clients and investors – carried interest documentation, contact details, know your customer (KYC) and related anti-money laundering information, subscription agreements and, potentially, side letters
- Employees – employment agreements, email address and contact details, next of kin and confidential medical history

Data processor

During the course of business, asset managers engage third parties who therefore become processors of personal data, such as:

- Accountants
- Companies engaged to store physical documents or dispose of confidential paperwork
- Fund administrators
- Fund distributors
- Lawyers
- Payroll firms
- Platform providers (e.g., wrapper – Individual Savings Accounts (ISAs) and self-invested personal pension)
- Technology vendors where data is not hosted on premises
- Outsourced back-office providers

Asset managers themselves are likely to be considered data controllers under GDPR, as they are determining the purposes and means of the processing of personal data. This means they are subject to wider legal obligations under GDPR due to their status as controllers.

The GDPR specifies six legitimate bases of processing personal data in Article 6:

1. Consent
2. Contractual necessity
3. Compliance with a legal obligation
4. Protection of vital interests
5. Public interest or official authority
6. Legitimate interests

The processing of personal data under GDPR is only lawful as long as at least one of the above mentioned legitimate bases applies.

Data controller

Wealth and asset managers themselves are likely to be considered data controllers under GDPR, as they are determining the purposes and means of the processing of personal data. This means they are subject to wider legal obligations under the GDPR due to their status as controllers.

Data processor

A fund's general partner, manager or administrator (as applicable) would likely be considered a processor. Alternative investment fund managers (AIFMs) and Undertakings for the Collective Investment of Transferable Securities (UCITS) funds, as well as fund umbrellas are likely to be data processors under the GDPR, acting on the documented instructions received from the data controller.

GDPR should not be seen as a mere compliance exercise – it offers the opportunity to implement best practice data protection protocols that safeguard your company's most valuable assets: your employees, your clients, your investors and your reputation.

Steps toward GDPR 2.0: how EY can help

EY broad transformation approach mirrors the cross-functional nature of the GDPR. We bring our own multidisciplinary teams of professionals, combining knowledge and experience specific to asset managers across legal, cybersecurity, and data analytics, to engage with stakeholders from all parts of the organisation, and to bring GDPR to life. Our five-phased GDPR compliance framework provides a tailored approach for each organisation, in order to operationalise GDPR, and support compliance as well as strategy beyond compliance.

EY's five-phased GDPR compliance framework

1. Understand

The business and governance models

Gather information related to the organisation and its adopted strategies to understand the current data protection governance model. Assess the industry and market, the organisation's management structure and its digital and data strategy, as well as the data protection measures and awareness in place.

Data protection and privacy framework

Leverage acknowledged frameworks, gather information and create an understanding of the existing data protection and privacy posture of the organisation, including policies, standards and guidelines.

Legal and regulatory framework

Understand the organisation's status and compliance toward the applicable laws and regulations, specifically GDPR and sector-specific laws and regulations.

Data transfers with vendors and partners

Understand the organisation's vendors and partners, including providers of cloud services and outsourcing. Create an overview of data transfers abroad, and understand the legal and regulatory impact.

2. Assess

Strategic alignment and risk appetite

Determine the strategic alignment and risk appetite in a workshop. Define the "tone at the top" toward strategy, risk culture, direction and conduct.

Data flow mapping

Map data flows to enhance the implementation support of data privacy. The identified data streams can be used to determine the requirements for privacy (on the basis of applicable laws and regulations) and setting up data protection.

GDPR maturity assessment

A tool-based privacy questionnaire is developed to assess the privacy maturity in different privacy domains, such as privacy strategy, data classification, etc.

Road map

The road map contains the necessary actions identified during the assessments and workshops. It will focus on compliance toward the applicable laws and regulations, and the defined privacy and data protection strategy.

3. Define

Privacy and data protection strategy

Develop an overarching strategy aligned with the business strategy and identified process improvements.

Governance, policy, standards and guidelines

Redefine the data protection governance model, including a detailed description of the roles and responsibilities with regard to management of external relationships and communication with regulators.

Data usage and flow mapping

Create an overview of where sensitive data flows within the organisation. Develop a data usage model based on legitimate use and consent as well as sustainable registration.

Data subject rights

Define processes to ensure data subject rights are enforceable. Facilitate compliance through privacy by design, e.g., embed user access rights in online applications. Evaluate and redesign processes for retrieval, correction and erasure of personal data throughout the organisation.

Data protection impact assessment and privacy by design

Assess personal data collection and processing activities with a data protection impact assessment to identify the risks inherent to the personal data processing activities. Reduce such risks by redefining the processes in accordance with the principles of privacy by design and privacy by default.

Vendor and partner management

Identify and prioritise the vendor relationships, which include personal data processing activities. Evaluate the contracts, security measures and oversight governance against compliance with GDPR and define a strategy to renegotiate personal data processing agreements. Ensure appropriate security measures and vendor management are in place by defining a lean oversight governance.

Monitoring and incident handling

Define a process for personal data breach monitoring and reporting. Develop a process for personal data breach reporting toward the data protection authority and toward the data subjects. Design templates and communication approval processes to ensure that the notification deadline of 72 hours can be met.

4. Recommend

Recommend the processes and measures defined in the previous phase 3, by leveraging existing processes within the organisation. Ensure data protection governance and documentation are in place by introducing internal guidelines and process documentations in order to comply with the accountability principle.

5. Run

Privacy control framework

Facilitate compliant personal data management through a holistic privacy control framework, integrating data protection throughout the organisation, including project management, process and product development, as well as risk and vendor management.

Raising awareness

Ensure data protection and privacy awareness through appropriate information, and specific data protection awareness trainings and workshops. Workshops will help stakeholders to understand that privacy is more than solely a compliance or security issue. Privacy game, case study and break out sessions form a part of the awareness workshops.

EY can help with managed services

- Web-based data protection trainings
- Data protection impact assessments
- Compliance monitoring
- Data breach stress tests

EY five-phased GDPR compliance framework

As GPDR straddles many areas of an investment firm – from HR to marketing, IT and sales – it is imperative to speak with key stakeholders about current practice and see what changes are necessary.

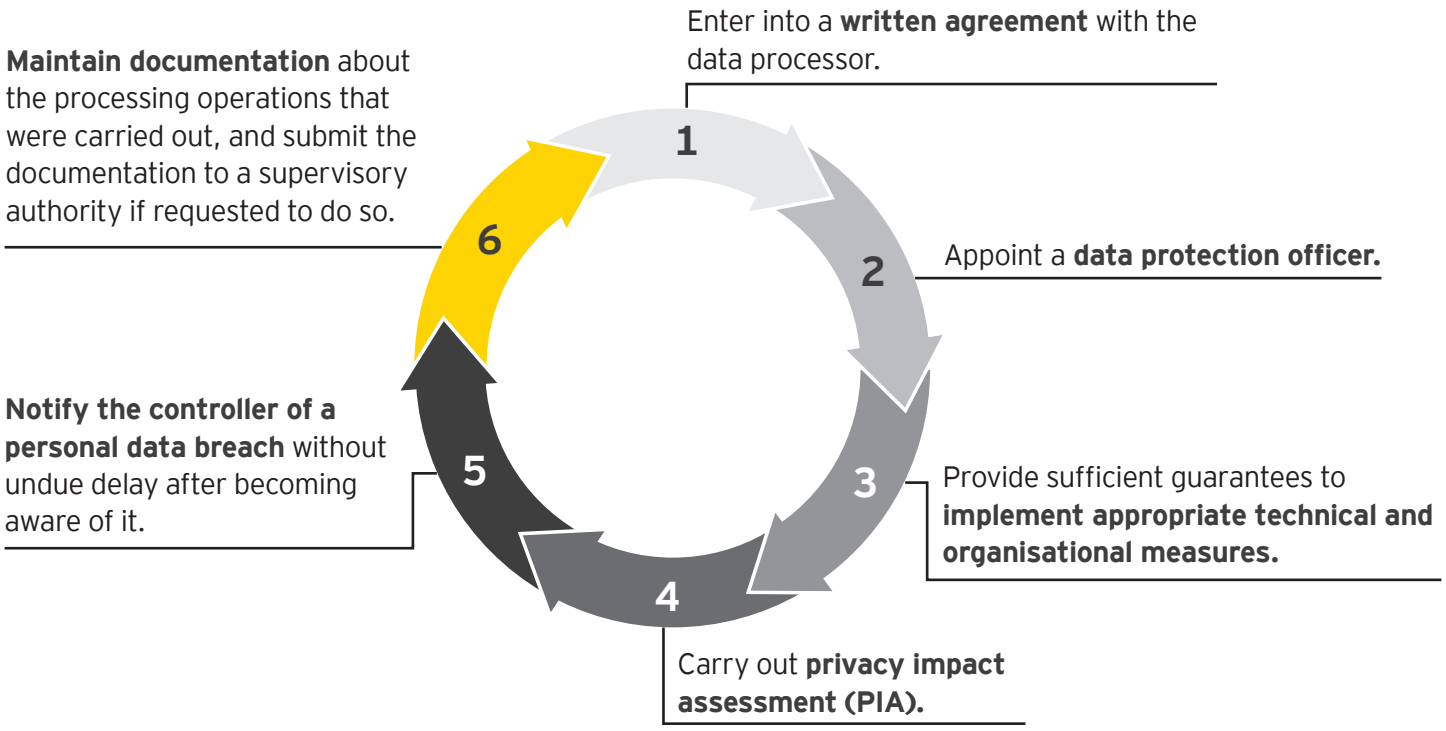
Our framework includes carrying out a data-mapping exercise, and putting in place appropriate documents and agreements with respect to any personal data, including employee and investor personal data that the fund manager processes.

As discussed, the concept of "privacy by design" is a key principle of GDPR. We suggest that you consider GDPR as a continuous virtuous cycle of data privacy:

We can help you implement a customised approach combining a GDPR maturity assessment and PIAs on high-risk data flows. EY's five-step framework not only supports customised GDPR compliance, but can also help increase the data maturity of the business as a whole – GDPR compliance programs often supports an optimisation of existing IT environments, in order to facilitate privacy across the whole IT domain. Two high potential areas are implementing robust Identify-Access-Management, and anonymising and pseudonymising data to supports analytics.

EY can help you apply these concepts to maximise the intelligence from data analytics, while supporting GDPR compliance.

Virtuous cycle of data privacy



Other GDPR services

EY can provide a wide range of GDPR services:

- Privacy strategy and governance
- Privacy design and implementation support
- Privacy impact assessment
- Dataflow mapping
- Managed services
- Privacy program and data management
- Privacy and data analytics, including anonymisation and pseudonymisation
- Maturity assessment
- Gap assessment
- Data breach notification and incident management
- Third-party and vendor management
- Training and awareness

EY Contacts

To discuss how EY can help you implement a customised approach to GDPR, please contact:

Lisa Kealy
Wealth & Asset Management,
Sector Leader
T: +353 1 221 2848
E: lisa.kealy@ie.ey.com

Paul Traynor
Partner and Advisory Lead,
Wealth & Asset Management
T: +353 1 425 5121
E: paul.traynor@ie.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

EYG No. 010643-18Gbl

EY-000070634.indd (UK) 08/18.
Artwork by Creative Services Group London.

ED None

In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/wealtham