SS&C | ADVENT®

General Data Protection Regulation

The implications for investment managers

WHITEPAPER

advent.com

By implementing it as a regulation, the GDPR aims to ensure the same data protection laws will apply uniformly across the EU. For the investment management industry, the new obligations will be extensive and challenging.

GDPR: Raising the data protection bar across the investment management industry

The General Data Protection Regulation (GDPR) has a clear goal: to introduce a higher, more consistent level of data protection across the European Union, which will give citizens back control over their personal data and simplify the regulatory environment for business[1]. The regulation, when it takes effect on May 25, 2018, will apply to all companies that hold or process EU residents' data, including asset and wealth managers and their service providers.

The existing framework of nationally-implemented legislation based on the EU Data Protection Directive has resulted in a lack of rule harmonization between member states. These variations, and at times conflicting rules, are complicating businesses' requirements and procedures, especially as data increasingly flows across borders in today's digital age. By implementing it as a regulation, the GDPR aims to ensure the same data protection laws will apply uniformly across the EU.

In addition, while many of the GDPR's concepts and principles build on those in the existing Data Protection Directive, the regulation introduces significant new rules and enhancements. The emphasis will be on how personally identifiable information (PII) is handled and protected by institutions within the EU—and, in certain cases, outside. For the investment management industry, the new obligations will be extensive and challenging.

Expanded scope

The GDPR applies to data 'controllers' (which say how and why personal data is processed) and 'processors' (which act on the controller's behalf). Where a processor is involved, controllers face stringent obligations to ensure their contracts with those processors comply with the GDPR.

The GDPR places specific new responsibilities on processors, making them "subject to the same compliance obligations, legal requirements, and punishment for non-compliance as controllers," notes EY[2]. These include maintaining records of personal data and processing activities. If a processor is responsible for a data breach, they will also be subject to much greater legal liability.

Within the investment management industry, investment funds and management companies will be deemed to be data controllers of investor data, notes a report by Dublin-based law firm Matheson[3]. A service provider acting on instructions from the fund or management company, as in an administration agreement, will likely be considered a processor, it adds. Having a clear definition of its remit, and not processing personal data outside the scope of the relevant contract will enable processors to avoid being designated a controller.

"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 (e.g. 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," notes the Matheson paper.

Furthermore, while current data protection rules focus on data controllers established in the EU, the GDPR also applies to non-EU controllers and processors that offer goods and services to, or monitor the behavior of, individuals in the EU.

[1] *Protection of personal data,* European Commission, http://ec.europa.eu/justice/data-protection/index_en.htm

[2] *When is privacy not something to keep quiet about?*, EY, September 2016, http://www.ey.com/Publication/vwLUAssets/ey-when-is-privacy-not-something-to-keep-quiet-about/$FILE/ey-when-is-privacy-not-something-to-keep-quiet-about.pdf

[3] *GDPR in Context: Impacts on the Asset Management Industry,* Matheson, May 2017, http://www.matheson.com/images/uploads/documents/GDPR_in_Context_-_Impacts_on_the_Asset_Management_Industry.pdf

Comprehensive governance measures, featuring more and better policies and procedures, should provide robust data protection and minimize the risk of breaches.

"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," says Matheson.

Core features

The GDPR institutes some far-reaching changes to EU data protection laws. Key elements include:

Accountability and governance

The most significant addition under the GDPR is the accountability principle, according to the UK's Information Commissioner's Office (ICO)[4]. This requires organizations to "show how you comply with the principles."

As such, notes Matheson, the GDPR imposes new requirements relating to the analysis and documenting of data processing activities.

To achieve and demonstrate compliance, firms must:

- Implement technical and organizational measures to ensure they comply, such as staff training to enable adherence to internal data protection policies and internal audits of processing activities.
- Maintain relevant documentation on processing activities, including a registry of all the personal data held in the company, explaining what is done with the information, and how it is used and secured.
- Appoint a data protection officer where the organization meets certain thresholds.
- Implement 'data protection by design' and 'data protection by default' measures, such as data minimization, pseudonymization and transparency.
- Conduct data protection impact assessments (DPIAs)—also known as privacy impact assessments—where there is a high risk to the rights and freedoms of individuals (for example, with profiling). DPIAs aim to help organizations identify and fix any problems, and meet their compliance obligations in the most effective way.

Comprehensive governance measures, featuring more and better policies and procedures, should provide robust data protection and minimize the risk of breaches.

Consent

"Consumer consent to process data must be freely given and for specific purposes," observes EY[5]. "They also must be informed of their right to withdraw their consent." In addition, there are new restrictions on children's ability to consent to data processing without parental authorization.

Data breach notification

A data breach is deemed to be the destruction, loss, unauthorized disclosure, alteration or access to personal data. Upon discovering a breach, data controllers must notify their national data protection authority within 72 hours. "The notification must include the nature of the breach, who had been affected, the potential implications of the breach, and the steps the organization has taken to address it," notes EY[6].

In cases, where there is a "high risk" to their rights and freedoms, the controller must also notify the affected data subjects without undue delay.

[4] *Overview of the General Data Protection Regulation (GDPR)*, ICO, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

[5] *EU General Data Protection Regulation: are you ready?*, EY, http://www.ey.com/Publication/vwLUAssets/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017/$FILE/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017.pdf

[6] *When is privacy not something to keep quiet about?*, EY

Figure 1: **Key responsibilities for the investment management community**

Controllers	Processors
Clearly communicate with data subjects regarding the processing of their personal data.	Process only on the documented instructions of the controller to avoid being designated a controller.
Obtain unambiguous consent and inform individuals of their rights.	Maintain accurate and detailed records of all processing activities carried out on behalf of each controller.
Implement appropriate technical and organizational measures.	Quickly notify controllers of any data breach.
Conduct due diligence on processors to ensure they can meet their obligations.	Appoint a Data Protection Officer where required.
Notify supervisory authorities and data subjects of relevant data breaches.	
Maintain more extensive records of processing activities in a data registry.	
Conduct data protection impact assessments where appropriate.	
Appoint a Data Protection Officer where required.	

Individuals' rights

The GDPR strengthens data subjects' rights through, for example:

- The right to be informed, which ensures there is transparency as to how organizations use personal data.
- The right of access to their personal data.
- The right to restrict processing, where firms are permitted to store personal data but not further process it.
- The right to data portability, which allows individuals to receive their personal data in a structured and commonly used format, so they can easily move, copy or transfer it to another data controller. A joint IAPP and EY report found financial services organizations expect this obligation to be particularly difficult[7].
- The right to erasure, also known as 'the right to be forgotten.' This enables an individual to request the deletion or removal of personal data in specific circumstances where there is no compelling reason for its continued processing.

"Data controllers will need to put in place clear processes to enable them to meet these obligations," notes international law firm Allen & Overy[8].

Liability and penalties

Data controllers will be held liable for damage caused by processing that infringes the GDPR. Data processors 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," according to Matheson.

Depending on the nature and gravity of the breach, fines for infringements of the rules range from €10m or 2% of total annual global turnover in the previous financial year (whichever is higher), up to €20 million or 4% of annual turnover. This marks a significant increase from the existing rules. For instance, analysis by NCC Group determined that if the GDPR formula had been applied, ICO fines against British companies in 2016 would have been £69m, instead of £880,500[9].

Alongside the monetary penalties, any data breaches or regulatory sanction could result in substantial reputational damage.

[7] IAPP-EY Annual Privacy Governance Report 2016, IAPP and EY, https://iapp.org/media/pdf/resource_center/IAPP%202016%20GOVERNANCE%20SURVEY-FINAL3.pdf

[8] *The EU General Data Protection Regulation,* Allen & Overy, http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

[9] *Last year's ICO fines would be 79 times higher under GDPR,* by John Leyden, The Register, 28 Apr 2017, https://www.theregister.co.uk/2017/04/28/ico_fines_post_gdpr_analysis/

For many industry participants, GDPR compliance has been left on the back burner, as attention focused on other business and regulatory priorities, not least MiFID II.

What does this mean for the funds industry?

GDPR requires a "programmatic approach to data protection," warns PwC[10]. Therefore, affected firms will need "a defensible program for compliance and to prove you're acting appropriately."

This will force asset and wealth managers, along with their service providers, to re-evaluate how and what data they store. As a result, firms will need to ensure they can:

- Limit who within the organization sees certain data.
- Report on who has seen a client's data.
- Meet any client requests for their personal data to be deleted.

But making the necessary changes raises a number of challenges.

Legacy applications

Among the myriad systems financial firms typically use, many applications will not have the functionality or flexibility to comply with GDPR. This particularly applies to the regulation's requirement that, where requested, firms be able to delete any personal identifying information. Having a multiplicity of interconnected systems, especially where they operate off relational databases, makes deleting a customer's data across the entire enterprise exceedingly complex.

Logging and reporting may be problematic too. In the past, locking down the data and maintaining permissions policies that determined who in an organization was allowed to see certain levels of client information was sufficient. Under GDPR, both data controllers and processors need not only to lock down the data, but be able to prove it. In addition, they must have the ability to report on who tried or has seen the data.

Where firms are using non-compliant applications, they may be forced to replace those, or no longer store personal information within them. Another option could be to depersonalize the information in those systems, so that clients are referenced by a code, rather than their personal data.

As ICO points out: "Personal data that has been pseudonymized—e.g. key-coded—can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual."

A further alternative, where feasible, could be to add functionality to the systems to allow the data to be encrypted, so that if a client requests their data be deleted, employees can no longer see it. Should access be needed subsequently—for example, if there is an audit or lawsuit—the data could then be de-encrypted.

Either way, replacing out-of-date systems, and consolidating applications into a more efficient and more integrated technology infrastructure, will make it easier for firms to control their data and comply with the regulation.

Regulatory conflicts

Multiple financial regulations (e.g. KYC and AML rules, MiFID II, client suitability and FATCA/GATCA) require firms to obtain and maintain detailed client information to ensure the person is who they say they are, that products and services are suitable to their circumstances, and prevent them from engaging in tax evasion. This emphasis on knowing clients and retaining data, for up to seven years in some instances, is at odds with the GDPR's focus on controlling who has access to the data and the right for a client's information to be deleted.

Again, encrypting the client information so it becomes effectively inaccessible to a firm's employees, while allowing it to be decrypted should a regulator demand, may be a way to square that circle. However, many of these conflicts and issues have not yet been challenged.

[10] *General Data Protection Regulation (GDPR),* PwC, https://www.pwc.com/us/en/cybersecurity/general-data-protection-regulation.html

Figure 2: **Key considerations on the road to compliance**

1	What new obligations does the GDPR introduce for organizations like yours?
2	How do your current policies and processes compare with the GDPR requirements? In particular: • How is personal data accessed and logged? • Who has access to what data within your firm? • Can you control and report on that data access? • What happens when a client asks for their data to be deleted? Is that possible? How many different systems does it entail? How can the process be simplified and guaranteed?
3	Can you make the necessary changes to ensure compliance using your existing systems infrastructure? If not, what enhancements/new applications will be required?

Permissions policies

Permissioning policies vary widely, depending on the type, size and culture of an individual firm. In some (typically smaller) institutions, client information may be widely held and easily accessible by all the firm's employees. Other organizations will lock down certain data and maintain strict permission rules.

Going forward, all firms will have to re-evaluate and prospectively tighten their in-house policies on how data is stored and who has access to it, shifting to a 'least privilege' model where access is strictly limited to staff who truly need the data to do their job. This means having the capability to set up and apply permissioning rules to allow or disallow access, log exactly who has seen what data and how they are accessing and sharing it, and then report back to the end client with that information. In addition, notes the Matheson paper, both controllers and processors will need to review, and where appropriate revise, all subscription agreements, prospectus disclosures, website terms, and service provider and data transfer agreements to ensure they meet the GDPR requirements before the regulation takes effect.

Action steps towards compliance

For many industry participants, GDPR compliance has been left on the back burner, as attention focused on other business and regulatory priorities, not least MiFID II.

Yet GDPR will introduce a significant strengthening of the data protection rules for both EU and affected non-EU firms. The regulation also raises the stakes by substantially increasing the penalties that can be applied for any rule breaches. Compliance is essential. And time is running short.

To help firms prepare, ICO has published a 12-point checklist[11] of the steps firms should be taking now:

1. Awareness

Ensure decision makers and key people within the organization are aware the law is changing and the impact the GDPR is likely to have.

2. Information you hold

Document what personal data you hold, where it came from and who you share it with. An information audit may be necessary.

3. Communicating privacy information

Review current privacy notices and plan to make any necessary changes (e.g. ensuring information is in clear and plain language) in time for the GDPR's start date.

4. Individuals' rights

Check your procedures to ensure they cover individuals' rights, including how you would delete personal data, or provide data electronically and in a commonly used format (the right to data portability).

5. Subject access requests

Update procedures and plan how to handle requests within the new timescales.

6. Lawful basis for processing personal data

Identify and document the lawful basis for your processing activity in the GDPR, and update your privacy notices to explain it.

7. Consent

Review how you seek, record and manage consent, and make any changes as required. Refresh existing consents if they don't meet the GDPR standard.

[11] *Preparing for the General Data Protection Regulation (GDPR)*: 12 steps to take now, ICO, https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Taking steps now to implement appropriate data policies and make the necessary system changes before the regulation comes into force next year therefore is essential.

8. Children

Determine whether you need systems to verify individuals' ages, and obtain parental/guardian consent for any data processing activity.

9. Data breaches

Ensure the right procedures are in place to quickly detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments

Familiarize yourself with the ICO's code of practice on PIAs and the latest guidance from the Article 29 Working Party. Work out how and when to implement them systematically in your organization.

11. Data Protection Officers

Designate someone to take responsibility for data protection compliance, and determine where this role will sit. Establish whether you need to formally designate a Data Protection Officer.

12. International

If you carry out cross-border processing, determine your lead data protection supervisory authority from the Article 29 Working Party guidelines.

A best practice framework for GDPR compliance

GDPR compliance demands a twin-pronged approach, combining updated in-house data policies that limit unnecessary data access, along with a technology infrastructure that enables users to set up and apply permissioning, and track and report internally and externally on who accesses that personal data.

In essence, that means that by May 2018, firms need systems functionality that allows them to:

Log access—Set up and track individual users' and, where required, user teams' access to personal data within the organization. The flexibility to apply and control different levels of access permission to individuals/teams is crucial.

View access logs—Have the functionality to see which users saw whose personal data, and how those users accessed it.

Validate permissions—When a user accesses a client's personal data, be able to easily validate the permissions that gave the user access.

Report to clients—Any time an end client inquires about the security of their data, your systems must be able to run reports that show how many times different user teams have viewed the client's data, and how they accessed it.

Delete personal data—Ensure your systems and procedures can locate and delete/encrypt the necessary personal data in line with the regulation's stipulations.

Conclusion

While the GDPR builds on EU member states' existing data protection frameworks, it will both harmonize those rules across the bloc for the first time, and raise the standard considerably. For the investment management industry in particular, the regulation will introduce areas of conflict and complexity. However, the prospective penalties—financial and reputational—for non-compliance will be severe. Taking steps now to implement appropriate data policies and make the necessary system changes before the regulation comes into force next year therefore is essential.

To learn more about the GDPR and how SS&C Advent can support your business, get in touch at advent@sscinc.com.

About us

With more than 4,500 clients around the world, from established global institutions to small start-up practices, SS&C Advent is a recognized technology leader in the investment management industry. We have been delivering unparalleled precision and ahead-of-the-curve solutions for more than 30 years, helping investment managers and fund administrators around the world to minimize risk, meet their compliance obligations, grow their businesses and thrive.

To learn more about the GDPR and how SS&C Advent can support your business, get in touch at advent@sscinc.com.

SS&C | SMART PEOPLE SUPERB TECHNOLOGY

advent.com | advent@sscinc.com