April 25, 2018

GDPR—One Month to Go: Considerations for US Asset Managers

Introduction—The EU General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR)[1] will become law in all European Union (EU) and European Economic Area (EEA) member states (including the United Kingdom, notwithstanding Brexit) one month from now—on May 25.

It significantly updates the current data protection regime in force across the EU and EEA, replacing the current rules governing the collection, storage and processing of personal data and all in-scope firms. All US asset managers providing/offering asset management services to EU/EEA-based investors/managed account clients, or who otherwise have EU/EEA-based persons on their mailing lists, need to ensure they are compliant by that date.

1. Key Definitions

- **"Data subject"** means any living identified or identifiable natural person. In an asset management context, this is most likely to be investors or clients (including both current and former clients and investors, as well as prospective investors and clients), or officers and employees of any EU/EEA-located affiliates of a US management company.[2]
- **"Personal data"** means any information relating to a data subject, who can be identified, whether directly or indirectly, from that information. For example, a share register, associated Know Your Client documentation, data and information on directors and employees of a management company.
- **"Data controller"** means any natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data, such as a management company or, in some circumstances, a fund administrator.
- **"Data processor"** means a natural or legal person that processes personal data on behalf of and in accordance with the instructions of a data controller, such as a fund administrator, distributor and/or other delegates that receive personal data from the data controller.

2. Why/How Does the GDPR Apply to US Asset Managers?

The GDPR aims to strengthen and unify data protection for all individuals located in the EU/ EEA by implementing more rigorous operational requirements for those processing and controlling personal data. The GDPR places obligations on asset managers who:

[1] The Regulation (EU) 2016/679, available here.

[2] In each case, if such individuals are in the EU/EEA.

For more information on GDPR compliance, please contact your Katten attorney, the firm's **Financial Services** group or any of the following authors.

In the UK

Neil Robson
+44 (0) 20 7776 7666
neil.robson@kattenlaw.co.uk

Alan Meneghetti
+44 (0) 20 7770 5232
alan.meneghetti@kattenlaw.co.uk

Christopher Hitchins
+44 (0) 20 7776 7663
christopher.hitchins@kattenlaw.co.uk

In the US

Wendy Cohen
+1.212.940.3846
wendy.cohen@kattenlaw.com

Doron Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Matthew Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

- have an office in the EU/EEA;
- offer goods and services (such as managed account management services or fund management) to individuals located in the EU/EEA (regardless of whether a fee is charged for that service); or
- monitor the behavior of individuals located in the EU/EEA.[3]

It is important to note that the GDPR's applicability is not determined by citizenship or legal residence, so it could apply to non-EU/EEA citizens who are in the EU/EEA or whose personal data is processed by entities subject to the GDPR.

3. Brexit: Will the GDPR Continue To Apply After the UK Leaves the EU?

Yes. As currently proposed in the UK's Repeal Bill[4], all direct EU legislation (including regulations such as the GDPR) shall, so far as it is operative immediately before the UK leaves the EU, be drawn into UK domestic law on and after Brexit day—unless explicitly repealed thereafter. Therefore, it is prudent to work on the basis that the GDPR will continue to apply in the UK for the foreseeable future.

4. What Obligations Do Asset Managers Have To Comply With?

US asset managers that fall within the scope of the GDPR (i.e., because they have EU/EEA-based clients or investors) will have to meet the full compliance requirements of the GDPR. These requirements will depend on whether a fund manager is a data controller or a data processor. Although an individual assessment should be carried out on a case-by-case basis, asset managers holding names or other personal data on EU/EEA data subjects will likely be data controllers (i.e., they will determine the purpose and means for which the personal data is processed).

Data controllers are obliged to communicate with data subjects regarding the processing of their personal data and their rights in relation to that processing. This can be achieved through enhanced disclosures—commonly by including a data protection notice or statement in the subscription documents and on the manager's website (ideally on the 'landing page' rather than behind a password protected portal). It is important that such communications are concise, easily accessible and transparent, using clear and plain language. It also is important to justify on what legal basis asset managers collect, process and store personal data and for what purposes.

US asset managers that are data controllers also will be obligated under the GDPR to ensure that not only do they only hold the relevant personal data necessary to perform applicable services, but to monitor the personal data they hold and delete it when it is no longer required by applicable law or regulation. The result is that in-scope managers should have in place an ongoing "rolling" process for assessing whether the data that is held is required to be held and, if not, whether/how to delete it.

GDPR-covered data subjects also have a right to request that asset managers delete their personal data (often referred to as the "right to be forgotten"), though the asset manager's legal and regulatory obligations take precedence. Asset managers should be aware that such obligations also apply to past/former clients and investors, and they should consider the personal data of past clients/investors as being as relevant under the GDPR as the personal data of current clients/investors.

5. A Compliance Case Study—US Asset Managers

How Should You Go About Complying With the GDPR?

A. **List the types of personal data that you process and record the sources of this data:** You may hold personal data relating to investors (current and past investors), clients, employees, counterparties, contacts and third parties authorized to act for investors.

---

[3] It should be noted that US managers that are not marketing in the EU/ EEA (so as to avoid filing obligations under the Alternative Investment Fund Managers Directive) and who rely on reverse solicitations from EU/EEA investors may still be in scope if they are monitoring their EU/ EEA investors and if they hold/control/process data on EU persons—since the GDPR regulates the processing of the personal data by individuals, companies or organizations relating to individuals in the EU/EEA. US managers should be aware that the GDPR gives EU/EEA data subjects more control over their data, for example by introducing the "right to be forgotten" and the right to request that their personal data be erased. Even if a firm considers itself outside scope, if it holds data on EU/EEA data subjects it should consider putting policies and procedures in place to deal with such requests

[4] In Formally known as the European Union (Withdrawal) Bill, available here.

- **Investors** have to provide a wealth of information when choosing to invest in a fund or establish a managed account with a manager, which usually includes basic details such as their name, date of birth and address. It also could include more commercially and financially sensitive information such as payment details, tax residence information and information about the source of funds. Much of this information will need to be collected, used in some way and retained or stored to fulfill contractual requirements or to comply with regulatory rules such as IRS record retention requirements, SEC investment adviser rules and US broker-dealer rules.
- **Contacts** may have provided data in the past that is now processed for marketing purposes.
- **Counterparties** located in the EU or EEA will likely transfer data to you in the US over the course of a transaction.
- **Service providers** in the EU/EEA also may have passed personal data to you—contact names and email addresses of EU/EEA distributors, brokers or other service providers is personal data within the scope of the GDPR.

B. **Draw up a list of the people to whom you send personal data:** Asset managers need to ensure that each party has assessed its own obligations, including third-party service providers (such as your lawyers, accountants, administrators, transfer agents, company secretary or investment managers), any supervisory board of directors and non-EEA counterparties.

C. **Establish the legal basis for lawfully processing the data identified:** While you may have obtained explicit consent for controlling and processing personal data for certain purposes, you may lawfully process personal data without consent if you have another legal basis for that processing. For example, the GDPR allows you to process personal data where you are subject to contractual and regulatory obligations to do so, as is the case with existing investors, and in certain limited circumstances you may be able to assert that you have legitimate interests in processing that personal data.

D. **Check third-party agreements to assess GDPR obligations:** This may include reviewing key documents such as fund subscription agreements, PPM disclosures, website terms and service provider or transfer agreements. Given that subscription documents already contain a US data privacy notice, it also may be beneficial to include a GDPR privacy notice where the subscription documents are to be used by EU/EEA investors.

E. **Create data handling, data breach and data retention policies:** A GDPR data privacy policy should be prepared and made available publicly (such as on a publicly available page of the manager's website). If you have an EU/EEA affiliate, you will need to prepare further internal policies, GDPR protection wording for agreements with third parties, as well as training for your EU/EEA-based staff on conducting regular audits, as well as meeting EU/EEA obligations and dealing appropriately with data incident responses.

F. **Review your IT security systems and record retention policies to demonstrate compliance under the GDPR:** Undertaking a review of the manager's risk dynamic for all forms of processing, as well as establishing/updating detailed information security policies and procedures covering both organizational and technical measures is highly recommended.

G. **Continue to review and evaluate ongoing compliance, addressing any new types of personal data processing that you undertake and ensure that you address new regulatory and legal developments:** Compliance with the GDPR is not a one-time event. Managers must ensure that as long as they are in scope of the GDPR they stay compliant, including observing any changes in best practice.

6. What Steps Should I Take Next?

Asset managers holding GDPR-subject personal data should ensure that they have gone through the process of deciding what data they actually need, mapping relevant data flows and determining the correct legal basis for any data processing. Failure to do so could lead to a regulatory investigation/audit by the relevant EU data regulator (such as the UK's Information Commissioner's Office) and, in circumstances where a firm fails to comply with the GDPR, could result in substantial fines by applicable EU or EEA data regulators. The GDPR provides for fines for non-compliance (including improper international personal data transfers) of up to the greater of €20 million (approx. $24.7 million) or 4 percent of the firm's aggregate (including all affiliates) annual global turnover.[5]

[5] It is acknowledged that enforcement of a fine raised by an EU regulator against a US asset manager with no EU subsidiary or other presence may present a legal challenge; however, in the current climate compliance with the GDPR is highly recommended.

7. Action Points

At a minimum, it is recommended that in-scope managers (and their various service providers processing personal information on EU/EEA data subjects) should carry out a GDPR compliance project as soon as possible, taking into account the following steps:

- Carry out a data mapping exercise. What personal data do you hold? What legal basis do you have for controlling or processing it? Do you need data subject consents?
- Ensure that data processing is limited to what the data was originally collected for and that only those personnel within the firm that need to access the personal data are able to do so.
- Put in place appropriate policies and procedures and agreements with respect to any personal data and investor data that you process, including, if relevant, employee data (e.g., if you have an EU/EEA affiliate, make sure that you review the relevant employment agreements and employee handbooks).
- If any personal data that you process is transferred to a non-EEA jurisdiction, ensure that country, territory or sector ensures an adequate level of protection substantially similar to that in the EU/EEA under the GDPR in relation to the processing of personal data; a mechanism to transfer that personal data will need to be put in place, such as a data transfer agreement based on GDPR model clauses or binding corporate rules.