Proskauer

GDPR: FAQ for Non-EU Fund Managers

The General Data Protection Regulation (the **"GDPR"**) comes into force automatically in each of the European Union Member States (**"EU"**) on 25 May 2018. Data protection regulation is not new, with the GDPR building on what is currently in place across the EU. The GDPR, however, seeks to align and bolster the data protection regime across the EU.

This FAQ sets out some of the key questions that non-EU fund managers (e.g., investment advisers based in the U.S.) should be considering to assess how the GDPR may impact them.

Part 1: Background

What does the GDPR do?

The GDPR will implement more stringent operational requirements for processors and controllers of personal data, including, for example, 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, and higher standards for data controllers to demonstrate that they have obtained valid consent for certain data processing activities.

The personal data that businesses (including fund managers) should consider include both employee and investor/client/customer data. Personal data is data relating to a living individual (whether or not they are an EU citizen)[1] (referred to as a "data subject" in the GDPR) who can be identified from that data (or from that data and other information in the business's possession). Personal data can include an individual's business email address and contact details. Personal data may be found in employment agreements, carried interest documentation, anti-money laundering information, subscription agreements and, potentially, side letters.

Controllers are those organizations or persons who control personal data – they determine the purposes for which the personal data is processed and decide what is done with it. Processors are those organizations or persons who process the personal data at the behest of the controller and in accordance with their instructions. They do not decide what happens to the personal data. Processing is defined broadly and encompasses most kinds of actions carried out with respect to the data, including obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, or deleting, transferring or disclosing the data.

Depending on the particular fund structure employed, a fund's general partner, manager and/or administrator (as applicable) would likely be considered a controller. It is also likely that the general partner or manager (as appropriate) would, in the ordinary course of business, engage third-party processors of personal data such as fund administrators, payroll firms, stock distribution agents, accountants, lawyers or companies engaged to dispose of confidential information.

[1] Coverage by the GDPR generally depends more on who the organisation is, what it does, and where, than on who the data subject is

Who does the GPDR apply to?

Broadly, the GDPR applies to controllers and processors established in the EU as well as controllers and processors not established in the EU where the activities the controllers or processors carry out either involve (i) offering goods or services (such as interests in the fund manager's funds) to data subjects in the EU, and/or (ii) monitoring data subjects' behaviors in the EU (e.g., online tracking). This change from the previous data protection legislation will significantly increase the extraterritorial reach of European data privacy legislation.

Why does this matter?

The GDPR significantly increases penalties for non-compliance beyond what is available under current law, with fines for non-compliance of up to the greater of EUR 20 million or 4% of the business's worldwide annual turnover. If an organization's privacy or data security measures fail to comply with the GDPR, the organization may be subject to actions taken by the data supervisory authority, which may lead to enforcement orders, fines or other liabilities, as well as actions from individuals which may lead to claims for damages.

What are some of the key changes?

There are a number of changes that will occur when the GDPR comes into force. We outline some of the key ones below.

Breach Notification:

- A data breach consists of *"accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".*
- Data controllers are required to notify the applicable data supervisory authority of certain data breaches without undue delay and, where possible, within 72 hours of awareness. A reasoned justification must be provided if this deadline is not satisfied.
- Data controllers may also be required to notify data subjects if the breach is likely to result in a "high risk" to the rights and freedoms of individuals. The notification should be without undue delay. A data supervisory authority may also require a data controller to notify the data subject.

Consent:

- Under the GDPR, there are more detailed conditions for using consent to enable data processing, namely consent must be *"freely given, specific, informed, and unambiguous".* In cases of sensitive personal data it must also be "explicit".
- The new requirements will make consent more difficult to rely upon as a valid basis for processing and transferring data. Other lawful bases to process personal data may be relied upon if possible, e.g., as part of the performance of a contract or for relevant legitimate interests.

Data Subject Rights:

- Data subjects will now have expanded rights including the right to port personal data between service providers (known as data portability) and the right to object to automated decision-making.
- Protocols for dealing with data subject complaints/objections/requests for rectification and erasure as well as to access data (i.e., subject access requests) have also been updated.

Data Protection Officers ("DPOs"):

- Some businesses will be required to appoint a DPO. A DPO must be an expert in GDPR data protection laws and practices.
- This obligation applies to (1) all public authorities, (2) entities whose core activities involve *"regular and systematic monitoring of data subjects on a large scale",* and (3) entities who conduct large-scale processing of special categories of personal data (e.g., race, religion, etc.). This is therefore unlikely to be applicable to most fund managers.

We should also note that although the GDPR seeks to harmonise data protection laws across the EU Member States, there are certain areas where EU Member States can increase protection, most notably with respect to employee data. Certain countries including Belgium, France and Germany have already made, or intend to make, use of this option.

Will Brexit mean that the GDPR will not be applicable to the UK?

No. The UK will be member of the EU when the GDPR comes into force in May 2018. The GDPR therefore will be directly applicable until such time as the UK formally leaves the EU. Even when the UK leaves the EU, it is likely that it will continue to apply the requirements of the GDPR to its domestic law. The prudent approach is therefore to work on the basis that the requirements of the GDPR will apply in the UK for the foreseeable future.

Part 2: GDPR and non-EU fund managers

What would bring non-EU fund managers in the scope of GDPR?

There are two ways a non-EU fund manager may be brought into the scope of the GDPR:

- If the non-EU fund manager has an establishment in the EU, then that establishment would be subject to the GDPR. The GDPR does not provide a definition of "establishment". Clearly a registered business in the EU is an establishment. However, the term is not likely to be interpreted so narrowly. The determination whether a business has an establishment in the EU must be determined based on the individual facts looking at the nexus of the business with the EU.
- If a non-EU fund manager does NOT have an establishment in the EU, but does either (i) offer goods or services (such as interests in the fund manager's funds) to data subjects in the EU, or (ii) monitor data subjects' behavior in the EU, then the non-EU fund manager may be subject to the GDPR. If the non-EU fund manager has no establishment in the EU, then the non-EU fund manager may need to appoint an EU representative.

This means, for example, if a non-EU fund manager does not have an establishment in the EU, and does not offer goods or services to data subjects in the EU or monitor data subjects' EU behaviors, then the non-EU fund manager may not be subject to the GDPR. Conversely, if a non-EU fund manager has an office in the EU and that office processes US citizens' data (whether or not those citizens live in the EU or U.S.), then that fund manager would need to comply with the GDPR with respect to the data held in the EU. However, on a practical note, if the US citizens are not living in the EU, and their data is merely being processed in the EU, this might not be an enforcement priority of data supervisory authorities (the governmental bodies appointed in each Member State to enforce data protection laws).

How will the GDPR impact non-EU fund managers if they are within the scope of the GDPR?

The non-EU fund managers who are within the scope of the GDPR would have to meet the full requirements of the GDPR. The organization should carry out a full GDPR compliance project, taking into account the next steps below. This would include carrying out a data mapping exercise and putting in place appropriate documents and agreements with respect to any personal data, including employee and investor data that the fund manager processes. In addition, if any personal data that the non-EU fund manager processes is transferred outside of the EU (including to the non-EU manager's home jurisdiction), then unless that country, territory or sector ensures an adequate level of protection 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 the model clauses or binding corporate rules.

A data transfer agreement based on the model clauses is a simple standard form, non-negotiable document that is approved by the EU Commission. Once signed, the contractual protections are considered adequate to allow the export of personal data from the EU.

Binding corporate rules are internal and legally binding rules for handling personal data. The rules must meet certain requirements and must permit data subjects to enforce their rights. Data supervisory authorities must sign off on the rules.

If a non-EU manager has no establishment in the EU, but the GDPR does apply in accordance with the above, will they be required to appoint a representative in the EU?

Once within the scope of the GDPR, non-EU managers are required to designate a representative in the EU unless: (i) the processing is occasional, (ii) does not include on a large scale processing of special categories of data (e.g., health data, data on trade union membership, race/ethnic data, criminal convictions or other offences), and (iii) is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing. For a non-EU fund manager that has EU investors, the crucial question is whether it is fair to say that their processing of the investor personal data is merely "occasional", given the frequency at which it communicates with the investors.

If an organization does designate a representative, this representative would represent the organization within the EU with respect to any obligations the organization has under the GDPR, including being the point of contact with data supervisory authorities and being a port of call for complaints from data subjects.

What next steps should a non-EU fund manager be taking to prepare for GDPR?

A non-EU fund manager should carry out the following:

- Determine the activities that they carry out either in the EU or in relation to data subjects in the EU.
- Map the personal data that they collect, store or process in the EU (including on any servers located in the EU) or in relation to data subjects in the EU, and determine what it is used for and how long it is kept.

Depending on the activities that the non-EU fund manager carries out and whether GDPR will apply to its activities, the following further steps may need to be taken:

- Review and update data protection policies and/or notices (this includes privacy policies employee data protection notices).
- Review and update agreements in relation to the transfer of data, including international transfers.
- Review and update service provider agreements and employment documentation.
- Review and update fund documentation to the extent necessary (e.g., consider the inclusion of provisions in the fund subscription agreement which refer to and/or include a privacy policy).
- Review information security policies.
- Review default data retention and erasure practices and policies.
- Consider the processes in place for handling data breaches and prepare a data breach policy/process.
- Train staff on data protection practices and breach.
- Consider whether an EU representative and/or DPO will need to be appointed (although DPO is unlikely to be necessary for the majority of fund managers).

Please contact the Proskauer Rose Data Protection Team for more information and to discuss how we can assist you in becoming GDPR-compliant.