



# General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) was published in May 2016 and becomes effective on 25 May 2018. It introduces a significantly enhanced EU data protection regime, replacing the EU Data Protection Directive (the Directive) which was drafted in the mid-1990s and was in urgent need of modernisation.

## Who is this relevant for?

---

The GDPR rules are relevant for all firms in the EU and many outside the EU. The rules apply directly to all organisations established in the EU, and any organisations established in a third country which process the personal data of natural persons located in the EU, and the processing relates to either: (i) offering goods and services to persons located the EU; or (ii) monitoring natural persons located in the EU.

## What does it cover?

---

The GDPR has the following main provisions relevant to alternative investment fund managers:

- **Legal grounds for processing personal data** – firms must have a legal grounds for every processing purpose for every piece of personal data for which they are a controller. These include: contractual necessity; legitimate interests of the firm; legal obligations; and consent. The GDPR, however, makes consent far harder to obtain and maintain for the purposes of processing personal data;
- **Data protection principles** – the GDPR requires compliance with seven principles for the processing of personal data including: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Firms must also ensure data protection in all processes 'by design' and 'by default'. This includes relevant cyber security measures;
- **Cross-border transfers** – firms must ensure that any personal data that is transferred from an EU entity to a third-country entity is undertaken in accordance with one of the permissible grounds under the GDPR;
- **Data subjects' rights** – data subjects are granted enhanced rights under the GDPR in relation to their personal data, including the: right to be informed; right of access; right to be forgotten; right to restrict processing; and right to object;
- **Use of third-party processors** – firms must ensure that if they rely upon third-party 'processors' of personal data for which they are a 'controller', that the processor guarantees compliance with the GDPR and contains certain minimum express provisions;
- **Data protection officers** – the GDPR requires firms that regularly and systematically monitor data subjects, or process sensitive personal data on a large scale, to appoint a 'Data Protection Officer' (DPO) compliant with the requirements of the GDPR;
- **Supervision, breaches and sanctions** – the GDPR grants greater oversight and sanctioning powers to supervisory authorities, and a requirement for controllers to notify material data breaches to supervisors within 72 hours of detection and to data subjects if the particular breach poses a high risk to them.

## Important future dates

---

The rules become effective on **25 May 2018**.

## Where can I find more information?

---

- [AIMA GDPR Implementation Guide](#)
- [General Data Protection Regulation \(GDPR\)](#)

Please contact AIMA's [Markets Regulation Team](#) for more detail on any aspect of the new rules.