Akin Gump
STRAUSS HAUER & FELD LLP

Financial Services Regulatory Alert

March 5, 2018

The Impact of the General Data Protection Regulation on Investment Managers

The new European[1] General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) will take effect on 25 May 2018. The GDPR expands and clarifies the EU's existing personal data protection framework. Investment managers will need to consider in good time what changes are necessary to their systems and processes to meet the GDPR requirements.

Scope

The existing data protection rules apply directly generally to EU investment managers who are data controllers. By contrast, the GDPR will apply to investment managers who:

- are established in the EU and are controllers or processors of personal data
- are established in a non-EU country and process personal data of data subjects who are based in the EU where the data processing activities are related to (i) the offering of goods or services to such data subjects in the EU or (ii) the monitoring of their behaviour as far as their behaviour takes place within the EU.

The processing of personal data under the GDPR is defined broadly and includes the collection, recording, organisation, structuring, storage, adaptation, disclosure by transmission, use or deletion of any information relating to a natural person. A "controller" under the GDPR will determine the purpose and means of the processing of particular personal data. A person who processes personal data on behalf of a controller will be considered a "processor".

Key Requirements Under the GDPR

Under the GDPR, controllers are subject to various prescribed requirements in respect of processing data and dealing with data subjects, including the requirement to:

- comply, and be able to demonstrate such compliance, with the "Principles" in both the planning and implementation phases of processing activities associated with a particular product or service
- communicate to data subjects in a concise, intelligible and easily accessible manner, and in clear and plain language, certain information regarding the processing of their personal data and their rights in respect of such processing
- notify the relevant national regulator of any data breach within 72 hours of becoming aware of the same for breaches that are likely to put rights of data subjects at risk, and, for high risk breaches, notify the data subjects without undue delay

- only appoint processors that guarantee compliance with the GDPR through a binding agreement in writing that meets the requirements prescribed by the GDPR (with additional requirements applicable where transferring personal data outside of the EU (e.g., model clauses))

Separately, and as a departure from the current data protection regime, the GDPR directly imposes on a processor a sub-set of the above requirements.

The "Principles" require, among other things, that personal data:

- be processed lawfully, fairly and in a transparent manner, and not be processed for any other purpose that is incompatible with that specified purpose, except where any specific exception applies
- be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- be accurate and, where necessary, kept up to date
- be kept in a form that permits identification of data subjects for no longer than is necessary for the processing purpose(s).

Penalties

All persons who have suffered damage as a result of an infringement of the GDPR have the right to receive compensation from either the controller or processor for the damage suffered (maximum of EUR 20 million or 4 per cent of global turnover for the most egregious breaches).

Next Steps

Investment managers will need to understand the types of personal data that they will likely be processing, and the different purposes for which the data may be processed, for example:

- employee data (including CVs, personal contact details, bank account details, performance records and background information)
- investor data (including data acquired in the process of conducting anti-money laundering checks on individual investors and directors/beneficial owners of corporate investors, and investor lists)
- portfolio company data (including data acquired in the process of conducting anti-money laundering checks, shareholder data, and employee and director data).

Investment managers will need to take steps to address the GDPR implementation, including assessing:

- all flows of personal data to, and from, the firm
- whether the way in which personal data is processed is consistent with the requirements under the GDPR (may require a review of general data security arrangements, data processing systems, investor documentation, staff privacy notice and transaction-related agreements (e.g. NDAs)
- whether the existing arrangements with data processors (including, for example, administrators, other service providers, advisers and group companies) are consistent with the requirements under the

GDPR, including the rules on the transmission of personal data outside of the EU (may require a review of each vendor service agreement).

Contact Information

If you have any questions regarding this alert, please contact:

Rosemarie Paul
rosemarie.paul@akingump.com
+44 20.7661.5313
London

Ezra Zahabi
ezra.zahabi@akingump.com
+44 20.7661.5367
London

[1] The GDPR will, in due course, apply in the EEA countries (Norway, Iceland and Liechtenstein), as well as the member states of the European Union.