

GDPR for US Investment Advisers

March 2018

The European Union is introducing a new piece of data protection legislation, the General Data Protection Regulation (GDPR), which will affect many US investment advisers. GDPR comes into force on 25 May 2018. In this note, we take a brief look at some of the key questions facing US investment advisers.

Simmons & Simmons has also published a more detailed briefing note on the implications of GDPR for UK hedge fund managers.

1. Are we subject to GDPR?

GDPR has extraterritorial effect. It will apply to a US investment adviser, and its funds, in three situations:

- (a) If fund interests or management services are offered to EU investors (see paragraph 2).
- (b) If it monitors the behaviour of individuals in the EU. This will most commonly happen through websites. Some investment advisers also use personal data in connection with their trading strategies, such as data on underlying borrowers or large-scale data used for algorithmic strategies.
- (c) If it has an establishment in the EU, such as a branch office, an affiliate or a marketing presence.

2. Are we “offering” our fund interests or services to EU investors?

This will often be a crucial test for US investment advisers. There will be an offering for GDPR purposes if it is “apparent” that the offering of fund interests or services to EU investors is “envisaged”, and GDPR cites factors such as the use of an EU language or currency in the offering, or references to EU customers. Even passive availability could therefore constitute an “offering” if there are indications that EU investors are specifically being accommodated.

It is not relevant whether the offering is made by the investment adviser or a third-party distributor – the question is whether the data processing is “related to” the offering, which in practice means that the processing of investor data will always be caught whenever there has been an offering to that investor.

Investment advisers that actively market their funds or services to EU investors (e.g. having registered their funds under AIFMD) will certainly be subject to GDPR with respect to the relevant data. Investment advisers relying on reverse enquiry in the EU may be able to remain out of scope, but should consider whether anything that they do or any feature of their fund could appear to envisage an offer to EU investors specifically.

On the face of it, offering to EU institutions, and not individuals, does not seem to trigger GDPR obligations, because the obligations only apply where the processing of an individual’s personal data is related to the offering of shares to that individual. The personal data of an institutional investor’s employee, for example, should therefore not be covered, on the basis that the offering is made to the institution and not to the employee. It is not yet clear whether data regulators will try to assert a more expansive interpretation of the text.

3. If there is an “offering”, which entity has to comply?

If a fund’s interests are being offered in the EU, then both the investment adviser and the fund will separately need to comply with GDPR.

In this case, GDPR only applies to the use of personal data on relevant EU individuals, although in practice this is likely to mean GDPR standards will be applied across all personal data on investors (e.g. regarding data security).

4. We have a group entity in the EU. How does that affect us?

The EU group entity will be subject to GDPR in its own right. That does not, in itself, mean that non-EU group entities are directly subject to GDPR, but they often will be affected. For example, if a non-EU group entity performs IT, HR or other functions for the EU group entity in a way that involves the processing of personal data, that non-EU entity is likely to be acting as a data processor for the EU entity and therefore be subject to GDPR in some respects.

Transfers of personal data out of the EU, including to affiliates, are also subject to certain conditions.

Depending on its activities, the EU group entity might also be deemed an “establishment” of the non-EU entity, which would bring the non-EU entity within the scope of GDPR. This will need to be considered on a case-by-case basis.

5. If we are subject to GDPR, what are our obligations?

If a US investment adviser or its non-EU fund is in-scope, it will need to comply with all of the requirements of GDPR in respect of the relevant personal data. These requirements include the following:

- (a) A GDPR-compliant data protection policy must be adopted (where proportionate)
- (b) The use of the data will be subject to various restrictions. In particular, GDPR specifies the only legal bases on which personal data may be used (e.g. consent has been obtained from the individual, or it is necessary for compliance with a legal obligation of the investment adviser or the fund, or it is necessary for the purposes of the investment adviser’s or the fund’s legitimate interests).
- (c) Detailed information must be provided to individuals, including information on the purpose for which personal data is used and the legal basis for doing so. A fund can provide this information to investors in its subscription documents, but an investment adviser will also usually need to provide the information itself as well, earlier in the process.
- (d) There are requirements relating to data security.
- (e) Records of data processing may need to be kept.
- (f) Agreements with fund administrators (and other service providers that process the relevant personal data – “data processors”) will need to be amended.

Individuals will also have the right to access their data, and in some cases to have it rectified, deleted or transferred, among other things.

6. What happens if we don’t comply?

The maximum fine under GDPR is the greater of €20 million (c. \$25 million) and 4% of worldwide annual turnover, which is potentially far more significant than any existing sanctions. However, most enforcement action by EU data regulators has historically taken the form of warnings, reprimands and corrective orders, the effect of which is primarily reputational.

While it seems unlikely that EU data regulators will focus on relatively small organisations such as investment advisers, any data security breach – especially a high-profile breach involving investor information – may provoke a regulatory investigation.

7. What are the next steps?

Investment advisers should consider the following steps:

- (a) Determine whether the investment adviser and its funds might be in scope.
- (b) If so, decide whether to comply with GDPR or rearrange matters so that they are not in scope (which may involve reduced access to EU investors).
- (c) If intending to comply, map the use of the relevant personal data – what it is, where it comes from, where it is stored, how it is used and why, and where it is transferred.
- (d) Update compliance processes and amend relevant documents.
- (e) Ensure data security is GDPR-compliant, not only at the investment adviser but also at any fund administrator or other relevant service provider.

Simmons & Simmons combines its market-leading European private funds practice with data protection specialists who have been advising asset managers on GDPR since its inception, and we would be happy to assist US investment advisers with their GDPR compliance issues.

Key contacts

For more information on GDPR, please contact any of the following:



Arthur Markham
Managing Associate

T +44 20 7825 4608
E arthur.markham@simmons-simmons.com



Lucian Firth
Partner

T +44 20 7825 4155
E lucian.firth@simmons-simmons.com



Devarshi Saksena
Partner

T +44 20 7825 3255
E devarshi.saksena@simmons-simmons.com



Richard Perry
Partner

T +44 20 7825 4310
E richard.perry@simmons-simmons.com



Iain Cullen
Partner

T +44 20 7825 4422
E iain.cullen@simmons-simmons.com



Sarah Crabb
Managing Associate

T +44 20 7825 3597
E sarah.crabb@simmons-simmons.com



Dale Gabbert
Partner

T +44 20 7825 3201
E dale.gabbert@simmons-simmons.com



Matthew Pitman
Partner

T +44 20 7825 4629
E matthew.pitman@simmons-simmons.com

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document. This document is subject to change.

elexica.com is the award winning online legal resource of Simmons & Simmons

© Simmons & Simmons LLP 2018. All rights reserved, and all moral rights are asserted and reserved.

This document is for general guidance only. It does not contain definitive advice. SIMMONS & SIMMONS and S&S are registered trade marks of Simmons & Simmons LLP.

Simmons & Simmons is an international legal practice carried on by Simmons & Simmons LLP and its affiliated practices. Accordingly, references to Simmons & Simmons mean Simmons & Simmons LLP and the other partnerships and other entities or practices authorised to use the name "Simmons & Simmons" or one or more of those practices as the context requires. The word "partner" refers to a member of Simmons & Simmons LLP or an employee or consultant with equivalent standing and qualifications or to an individual with equivalent status in one of Simmons & Simmons LLP's affiliated practices. For further information on the international entities and practices, refer to simmons-simmons.com/legalresp

Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS. It is authorised and regulated by the Solicitors Regulation Authority.

A list of members and other partners together with their professional qualifications is available for inspection at the above address.