Simmons & Simmons

GDPR for UK Hedge Fund Managers

March 2018

The European Union's General Data Protection Regulation (GDPR) comes into force on 25 May 2018. GDPR will extend the data protection responsibilities of UK and other EU hedge fund managers, and will also extend the direct application of EU data protection law to non-EU entities, including many funds. This note addresses how certain provisions of GDPR will affect the UK hedge fund industry.

Simmons & Simmons has analysed and identified the documents that managers ought to consider amending or putting in place for funds and for businesses such as asset managers, and has prepared template documentation for these purposes. Simmons & Simmons has also published a separate briefing note for US hedge fund managers.

1. What does GDPR cover?

GDPR, like the existing EU data protection regime, covers the use, storage and transfer ("processing") of information on identifiable individuals ("personal data"). In the hedge fund context, that includes personal data on investors and investor personnel, on employees, on individuals at service providers, peers, industry bodies, regulators and other organisations, and on website users.

Persons that determine the purpose and means of data processing, termed "controllers", are subject to the main bulk of regulation under GDPR. A manager will generally be a controller of the personal data that it holds, including that relating to investors and potential investors. A fund will also, separately, be a controller of the personal data that it holds on investors.

At a high level, a controller's obligations include: a requirement to have a data protection policy, where proportionate; restrictions on the processing of personal data (described in more detail below under "Legal basis for processing data"); obligations to provide individuals with certain information; obligations relating to the security of personal data; and requirements to keep records of data processing.

Persons that process personal data for purposes and by means determined by others are termed "processors", and are subject to fewer direct obligations. Service providers such as fund administrators and outsourced providers of certain IT and HR services will be processors in respect of many activities. The agreement under which a processor is appointed must include provisions regulating the use of data by the processor, and so it will be necessary to amend the relevant agreements.

2. The territorial scope of GDPR

One of the main changes being introduced to EU data protection law by GDPR is to its territorial scope. Many non-EU organisations will be subject to GDPR.

2.1 UK managers and their EU funds

All UK-based managers will be fully subject to GDPR by virtue of their establishment in the EU. The same will be true of any funds that they manage that are established in the EU.

In both cases, because the entity is established in the EU, GDPR will in effect apply in respect of all personal data that they process, whether it relates to EU individuals or non-EU individuals.

2.2 Non-EU funds: establishments

A non-EU fund will be subject to GDPR if it is considered to have an "establishment" in the EU. The key question is whether an EU manager will constitute an establishment for this purpose. While the matter is open to interpretation, it would generally be prudent to take the view that it does.

2.3 Non-EU funds: offerings of fund interests

If a non-EU fund does not have an EU establishment, it could still become directly subject to GDPR if interests in the fund are being offered to EU investors. GDPR's concept of an "offering" is broader than similar concepts relating to fund marketing, such as "marketing" under AIFMD or a "financial promotion" under the UK

regime, so that even the passive availability of fund interests could constitute an "offering" if EU investors are specifically being accommodated.

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 should therefore not be covered, on the basis that the offering is made to the institution and not the employee. It is not yet clear whether data regulators will try to assert a more expansive interpretation of the wording.

2.4 Non-EU affiliates

Managers with an affiliate outside the EU will need to consider a number of questions to determine the impact of GDPR on the affiliate:

(a) Does the non-EU affiliate have an "establishment" in the EU? Depending on the circumstances, an EU group entity such as the UK manager could constitute an establishment for this purpose.

(b) Does the non-EU affiliate offer "goods or services" to EU individuals? Fund interests and management services will qualify, as discussed above under "Non-EU funds: offerings of fund interests".

(c) Does the non-EU affiliate monitor EU individuals? It may do this through a website, for example.

(d) Does the non-EU affiliate process relevant personal data on behalf of any EU affiliates or funds (or other entities subject to GDPR)? If so, it may be acting as a "data processor" for an in-scope data controller.

(e) Does the non-EU affiliate receive personal data from in-scope data controllers for its own purposes? Receiving such data will not in itself make it directly subject to GDPR, but there may be indirect effects, such as a requirement to agree certain contractual terms.

3. Investment strategies

Some managers use personal data on individuals as part of their trading strategies. If this information is personal data, then the activity will be subject to GDPR. This may be the case if, for example, data on underlying borrowers is obtained or if information on large numbers of individuals is used for systematic strategies. In the latter example, if aggregated data sets are acquired from third parties then it may be the case that no individuals are identifiable, and so the data is not "personal data" for the purposes of GDPR.

Compliance with GDPR in these scenarios is potentially most problematic with respect to the requirement to provide specified information to all data subjects. However, the obligation does not apply if "the provision of such information proves impossible or would involve a disproportionate effort". This may often be the case in practice, although the point will need to be considered carefully.

4. Legal basis for processing data

Under GDPR, it is only permissible to process an individual's personal data where a specified legal basis applies. GDPR sets out the list of possible legal bases, the most important of which are the following:

Consent: Data processing is permitted where the individual has consented to the data being processed for the relevant purpose. The requirements for obtaining consent under GDPR are significantly more prescriptive than is currently the case. Obtaining appropriate consents from all investor-related individuals who provide personal data for AML purposes – most of whom will not sign the application form – will be difficult, and an individual can withdraw his or her consent at any time. Funds will therefore want to avoid having to seek consent for processing by ensuring that another legal basis can be relied on. Managers may, however, need to obtain consent for certain purposes, including some marketing activities.

Legal obligation: Data processing is permitted where it is "necessary for compliance with a legal obligation to which the controller is subject". This might, for example, cover the use of data for anti-money laundering purposes or disclosures relating to the automatic exchange of tax information. It does not include contractual obligations or obligations not recognised under EU law.

Legitimate interests: Data processing is also permitted where it is "necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject". While this justification has limits – the processing must be "necessary" and the interests of the controller must be balanced against the rights of the individual – it will nevertheless allow the processing for a wide range of ordinary business purposes without the need to obtain consent. In particular, funds should generally seek to do all of their data processing (including that done by their administrators) on this basis. Managers will also be able to do significant amounts of data processing on this basis, although, as noted above, it might not be justified in relation to certain marketing activities.

As well as needing a specific legal basis, all data processing must comply with a set of data protection principles. These include fairness, transparency, data minimisation, accuracy, confidentiality and accountability.

5.Transferring data outside the European Union

For the transfer of personal data to recipients outside the EU, GDPR requires one of a specified set of conditions to be met. The following conditions are most likely to be relevant:

Adequacy decision: A transfer can be made if the EU has determined that the target jurisdiction ensures an adequate level of protection for personal data. So far this only applies to a handful of jurisdictions (including Switzerland, Jersey and Guernsey), although other jurisdictions, including the Cayman Islands, intend to introduce local regulations with the intention of seeking an adequacy decision. The UK might seek to benefit from such a decision after Brexit.

Model clauses: A transfer can be made if standard clauses, approved by the EU, have been agreed between the transferor and transferee. Where no other condition can be satisfied, this will often be the fallback approach.

Binding corporate rules: A transfer can be made if legally binding rules, enforceable by the relevant individuals, are in place between the entities of a corporate group and have been approved by the relevant data regulator. This could be an appropriate arrangement to put in place for intra-group data flows.

Codes of conduct: A transfer can be made if the recipient has made a binding and enforceable commitment to abide by a code of conduct approved by the EU. Although no such codes of conduct are currently in place, it is possible that this will become a more useful option in the future.

The fact that another jurisdiction has imposed a legal obligation to transfer the data to it is not sufficient for the purposes of GDPR, unless the obligation is enforceable in the EU pursuant to a relevant treaty. Where managers or funds believe they might be subject to such an obligation, they should ensure that one of the other conditions for the transfer will be satisfied.

It is possible to transfer personal data outside the EU if an appropriate consent has been obtained. But, as with consent for general processing activities, this may be difficult to obtain consistently in practice.

Transfers of personal data – regardless of the location of the recipient – will also constitute "processing", and so will be subject to the need for a legal basis and to the data protection principles described above. Managers and funds should also be mindful of any duty of confidentiality.

6. Data security

Data security is already an issue of significant importance for managers, but GDPR adds two further layers.

Firstly, GDPR includes requirements relating to data security. Managers will therefore need to ensure that their data security measures – and those of fund administrators and other processors – are GDPR-compliant.

Secondly, a loss of personal data by a manager or by a fund's administrator is, for a hedge fund manager, the event that seems most likely to bring regulatory attention and scrutiny. Even if a manager has adequate data security, other deficiencies in the handling of personal data might come to light as a result of a data breach, resulting in sanctions being imposed.

7. Enforcement, penalties and data security

The maximum fines for breaches of data protection law will increase from £500,000 (in the UK) to the greater of €20 million and 4% of a group's worldwide annual turnover. 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.

Data regulators will also have increased powers and resources for proactive investigations. It seems unlikely that EU data regulators will focus on relatively small organisations such as hedge fund managers, as they will mainly be monitoring large consumer-facing businesses such as tech companies, supermarkets and banks. However, the examples of the Panama Papers and the Paradise Papers show that data breaches in the financial services sector are newsworthy, and regulators are likely to respond to a similar data breach by a manager or a fund administrator.

8. The impact of Brexit

The UK will cease to be subject to EU regulations such as GDPR when it leaves the EU on 29 March 2019, although the withdrawal agreement is likely to extend the effect of EU law for a transitional period.

Thereafter, the UK's European Union (Withdrawal) Bill and Data Protection Bill, both of which are currently passing through the UK Parliament, are expected to effectively incorporate GDPR into UK law after Brexit. While the core obligations are expected to be largely unaffected, different considerations will necessarily apply to cross-border transfers between the UK and the EU.

9. Next steps

Simmons & Simmons combines its market-leading UK hedge funds practice with data protection specialists who have been advising asset managers on GDPR since its inception, and we would be happy to assist managers 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