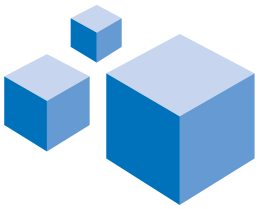

CUMMINGS

lawyers for alternative investments

General Data Protection Regulation – mandatory legal agreements between controllers and processors

www.cummingslaw.com | +44 (0)20 7585 1406

General Data Protection Regulation – mandatory legal agreements between controllers and processors

Introduction

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), enacted on 25 May 2016, replaces the EU Data Protection Directive (Directive 95/46/EC) (EU Directive). As an EU Regulation, the GDPR has direct effect in each EU member state without the need for further implementing legislation. It will take effect on 25 May 2018.

The GDPR introduces a single legal framework across the EU for handling personal data. While many of the EU Directive's core principles and obligations remain unchanged under the GDPR, the GDPR does impose new and additional requirements. One of the main changes is a new obligation to demonstrate compliance with the GDPR.

This Legal Long is the first in a series of three client briefings on the GDPR and will focus on the contractual arrangements which need to be in place between controllers and processors in order to comply with the GDPR.

Our two further Legal Longs will look at: (i) the impact on funds and fund documentation; and (ii) the impact of other provisions of the GDPR on those in the investment arena.

What are controllers and processors?

A controller is a natural or legal person, public authority, agency or any other body processing collecting and managing personal data. Data controllers determine the purpose and means of the processing of personal data.

A processor is a natural or legal person, public authority, agency or any other body processing personal data on behalf of a controller.

Who, in a fund structure, will be controllers and processors?

There are a number of different entities in a fund structure and it is possible that the work they carry out may lead them to be both controllers and processors.

It is important to look at the fund structure as a whole and establish the exact activities of each party to the arrangements to consider in which role and how responsibilities are divided and then agreed by contract.

As this is an EU directive, it is crucial that, as part of their analysis, the parties consider the jurisdiction of each relevant entity and whether they sit inside or outside the EEA. The GDPR prohibits transfers outside the EEA to processors unless the European Commission has determined that the third country (or international organisation) has an adequate standard of data protection. On 18 October 2017 the European Commission published the results of its first annual review of the EU US privacy shield and found it to provide adequate protection.

In addition, the parties may be both in relation to activities which are both internal and external.

To give some examples of how the roles of controller and processor may apply within the fund industry:

(i) investment managers will need to carry out know your client and anti-money laundering checks on both prospective investors and investors. This will involve gathering personal data which they will store and have control of, thus in this respect they will be controllers;

(ii) investment managers will also have employees and hold personal data on their employees and will therefore be a controller

in relation to their internal, commercial arrangements;

(iii) administrators will receive large volumes of information from investment managers which they will then process, as a processor. However, if the administrator goes beyond the scope of processing and determines the purpose and means of processing personal data, it will be treated as a controller in relation to that particular circumstance; and

(iv) distributors will have to follow their own FCA requirements in client identification and thus may gather information in respect of which they will be a controller, or may process information which has been gathered and controlled by the investment manager. Of particular importance in this situation is the interaction of the GDPR with MiFID II rules concerning manufacturers and distributors of investment products and their need to consider target markets and provide a flow of information between them.

What is personal data?

For the purposes of the GDPR, "personal data" means any information relating to

(i) an identified or identifiable natural person ("data subject"); and

(ii) an identifiable person is one who can be identified, directly or indirectly, by a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

What, in a fund structure, will be personal data?

To give two examples:

(i) hedge funds and fund managers are required by legislation relating to regulated activities and anti-money laundering to collect information on investors. Much of this will be, and will need to be, information which identifies people and will therefore be personal data; and

(ii) fund managers who are required to comply with rules on transaction reporting under MiFID II will also find themselves required to gather data on individuals within sell-side organisations which can be used to identify the individual broker and which is therefore personal data and subject to the GDPR.

How does a controller appoint a processor?

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected. In order to ensure this obligation is met, controller and processor relationships must be governed by a contract (or other legal act) under applicable law that binds the data processor and which is compliant with the rules set out in article 28 of the GDPR ("an Article 28 Agreement").

It should be noted that a while a processor may engage another processor, it is not entitled to do so without the prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

What must be in an Article 28 Agreement?

An Article 28 Agreement must be binding on the processor with regards to the controller and must set out:

(i) the subject-matter and duration of the processing;

(ii) the nature and purpose of the processing;

(iii) the type of personal data and categories of data subjects; and

(iv) the obligations and rights of the controller.

Article 28 (3) of the GDPR sets out the specific obligations of the processor, which are the bare minimum required, and are as follows:

(i) it must only act on the written obligations of the controller;

(ii) it must ensure that people processing the data are subject to a duty of confidentiality;

(iii) it must take appropriate measures to ensure the security of the processing;

(iv) it must only engage sub-processors with the prior consent of the controller and under a written contract;

(v) it must assist the controller in allowing data subjects to exercise their rights, including access, under the GDPR;

(vi) it must assist the controller in meeting its obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

(vii) it must delete (subject to local law) or return all the personal data to the controller at the end of the contract; and

(viii) it must make available to the controller all information necessary to demonstrate compliance with the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

How do I demonstrate compliance with the GDPR and Article 28?

In order for a controller to be able to demonstrate that it has complied with its obligations, Article 28 sets out some suggested policies and procedures, including but not limited to:

(i) policies and procedures for conducting due diligence on potential data processors, including screening questionnaires;

(ii) due diligence reports or data processor risk assessments;

(iii) data protection requirements for data processors;

(iv) policies and procedures for engaging data processors and executing contracts;

(v) privacy and security clauses for insertion into data processor contracts;

(vi) executed contracts with third parties that comply with Article 28 or include standard contractual clauses approved by the European Commission or other supervisory authority, once these standard clauses have been published; and

(vii) evidence of the data processor's adherence to an approved code of conduct.

How can we help?

Any contracts in place on 25 May 2018 will need to meet the new GDPR requirements. You should therefore check your existing contracts to make sure they contain all the required elements. If they do not, new contracts will need to be put in place or current contracts amended.

We are able to assist by carrying out a review of a firm's contractual arrangements and we can help re-draft or negotiate revised documentation.

If you would like our assistance in this respect, please contact us on the email addresses and telephone numbers set out below.

NOVEMBER 2017

Contacts

Claire Cummings

T: +44 (0) 207 585 1406
claire.cummings@cummingslaw.com

Christina MacLean

T: +44 (0) 207 585 1406
christina.maclean@cummingslaw.com