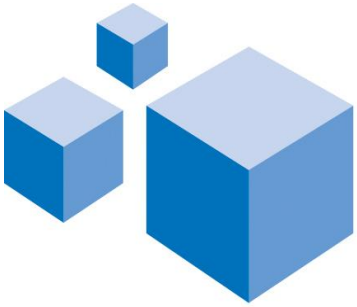


CUMMINGS

lawyers for alternative investments

The GDPR – how to prepare
MiFID II – where are we now?

Wednesday 21 February 2018

GDPR so far

- The EU General Data Protection Regulation (Regulation (EU) 2016/679) comes into effect on 25 May 2018
- Aims to protect: (i) natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and (ii) fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data
- Replaces the EU Data Protection Directive (Directive 95/46/EC) (EU Directive)
- Has direct effect in each EU member state without the need for further implementing legislation
- A single legal framework across the EU for handling personal data
- Article 29 data protection working party guidelines

CUMMINGS
lawyers for alternative investments

Key terms

- Controller - *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*
- Processor - *a natural or legal person, public authority, agency or any other body processing personal data on behalf of a controller*
- Personal data - *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*
- Consent - *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*
- Which entity has which role(s) in a fund structure?
- How do investors give consent to the right entities in a fund structure?

Territorial scope

- The processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

- The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

  (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

  (b) the monitoring of their behaviour as far as their behaviour takes place within the Union

- Personal data may only be transferred outside of the EU in compliance with specified conditions

- Countries with adequate levels of protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework). Ongoing talks with Japan and South Korea

- Derogations on transfer exist, for example where transfer is necessary for contractual reasons

- Offshore funds? Non-EEA administrators and brokers?

CUMMINGS
lawyers for alternative investments

Processing of data

- Specific principles apply to the processing of data:
  - lawfulness, fairness and transparency
  - specified, explicit and legitimate purposes
  - adequate, relevant and limited to what is necessary
  - identification of data subjects for no longer than is necessary
  - processed in a manner that ensures appropriate security
- Controllers are responsible and must be able to demonstrate compliance
- Who is a controller in a fund structure?
- How do investment managers meet their responsibilities?

CUMMINGS
lawyers for alternative investments

Legal obligations on Controllers and Processors

- Processors have specific legal obligations:
  - provide guarantees of ability to comply
  - maintain records of personal data and processing activities
  - liability for breach, including by a sub-processor
- Controllers, including joint controllers, have specific legal obligations
  - required to ensure contracts with processors are GDPR compliant
  - take into account the nature, scope, context and purposes of processing **and** the rights and freedoms of natural persons
  - implement safeguarding measures
- Article 28 agreement required between controllers and processors

Consent

- A key issue and must be *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data of him or her"*
- A positive opt-in and not consent by default
- Keep separate from terms and conditions
- Details of services and third parties
- Lawfulness heads include:
  - necessary for the performance of a contract
  - necessary for compliance by the controller
- Consider lawfulness in an industry in which personal data is a requirement
- Consider the relationship between investors and investment managers and the need for consent
- FCA and ICO update*: "the GDPR does not impose requirements that are incompatible with the rules in the FCA Handbook"*

Rights of individuals

- The right to be informed
  - what and when depends on how the personal data was obtained (see later slide on Privacy Notice)
  - specific details on the information to be given
  - where and how to be given in the context of a fund
- The right of access
  - must be free of charge
  - confirmation that data is being processed
  - personal data and supplementary information
- The right to rectification
  - inaccurate or incomplete

Rights of individuals

- The right to erasure (see later slide)
- The right to restrict processing
  - individual contests the accuracy (consider legitimate grounds override)
  - unlawful and the individual requests restriction not erasure
  - no longer needed but the individual requires to establish, exercise or defend a legal claim
- The right to data portability
  - move, copy or transfer personal data in a safe and secure way and only sometimes applicable
- The right to object
  - "grounds relating to his or her particular situation"
  - halt unless compelling legitimate grounds or legal claims
- Rights in relation to automated decision making and profiling

Right of erasure

- Personal data may be erased in certain circumstances:
  - no longer necessary or consent withdrawn
  - objection coupled with no overriding legitimate interest for continuing
  - unlawfully processed or to comply with a legal obligation
- Erasure or encryption equivalent?
- Requests for erasure can be refused:
  - right of freedom of expression and information;
  - exercise or defence of legal claims

Privacy Notice

- Fair processing obligation and transparency
- Concise, transparent, intelligible and easily accessible, clear and plain language and free of charge
- Consider who will control and process personal data and existing fund documentation
- Different information depending on source of supply – direct or indirect
  - ➢ directly – categories of personal data not required
  - ➢ indirectly – whether contractual requirement not required
  - ➢ both – controller's identity and contact details; purpose and lawful basis; any recipient; third country transfers and safeguards; data subject's rights; automated decision making
- Different time scales:
  - ➢ directly – at the time the data was obtained
  - ➢ indirectly – within a reasonable period (one month)/first communication if to subject/before disclosure if to another recipient

Article 28 Agreement (i)

- Binding on the processor with regards to the controller
- Must set out:
  - the subject-matter and duration of the processing
  - the nature and purpose of the processing
  - the type of personal data and categories of data subjects
  - the obligations and rights of the controller

Article 28 Agreement (ii)

- Article 28 (3) sets out the specific obligations of the processor, which are the bare minimum required:
  - only act on the written obligations of the controller
  - ensure that people processing the data are subject to a duty of confidentiality
  - take appropriate measures to ensure the security of the processing
  - only engage sub-processors with the prior consent of the controller and under a written contract
  - assist the controller in allowing data subjects to exercise their rights, including access, under the GDPR
  - 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
  - delete (subject to local law) or return all the personal data to the controller at the end of the contract
  - make available 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

Data Processing Officer (DPO); design and default

- A DPO must be appointed by entities which:

  (i) are a public authority (except for courts acting in their judicial capacity);

  (ii) carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or

  (iii) carry out large scale processing of special categories of data or data relating to criminal convictions and offences

- DPO must be independent and report to the highest management

- Design general obligation - to implement technical and organisational measures to show that data protection has been considered and integrated into processing activities

- Data processing:

  - should be limited to what is necessary for the purpose for which the data was collected

  - Accessed only by those within an organisation who need access to personal data

- Voluntary certification where able to demonstrate compliance with the principles of design and default

Breaches

- "… a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals"

- Report breaches to the ICO within 72 hours a description of the nature of the personal data breach

- Report breaches where they are likely to result in a high risk of adversely affect the individual's rights and freedoms to the individual without undue delay

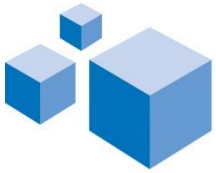
  - the categories and approximate number of individuals concerned
  - the categories and approximate number of personal data records concerned
  - the name and contact details of the data protection officer (if your organisation has one) or other contact point
  - description of the likely consequences and of the measures taken, or proposed to be taken, including to mitigate any possible adverse effects

- Fine up to EUROS 10 million or 2% of global turnover

CUMMINGS
lawyers for alternative investments

MiFID II – where are we now?

- December 2017 - The Financial Services and Markets Act 2000 (Markets in Financial Instruments) (No 2) Regulations 2017 (SI 2017/1255)
- February 2018 – FCA report on algorithmic trading compliance in wholesale markets
  - ➢ define algorithmic trading
  - ➢ develop and test, including risk controls
  - ➢ governance and oversight
  - ➢ market conduct
- ICE Futures Europe, the LME and Eurex granted exemptions from the open access regime until 2020
- ICE statement - 245 futures and options contracts in North American oil and natural gas liquids to move to ICE Futures U.S. instead of ICE Futures Europe in February 2019



CUMMINGS

lawyers for alternative investments

Cummings Law Ltd
42 Brook Street
London W1K 5DB

+44 20 7585 1406

www.cummingslaw.com

http://vimeo.com/cummingslaw