ACAMS Briefing 2nd May 2018

Agreements under GDPR
Countdown to GDPR

From May 2018

- GDPR - Regulation (EU) 2016/679 : Directly effective in all Member States including Ireland from 25 May 2018 – Overhauls the existing data protection regime relating to the protection of the personal data of individuals.

- In Ireland the Data Protection Bill 2018 (text published 1 February 2018) will –
  - Provide for derogations available under GDPR (e.g. S.44 proposes health data may be processed for insurance purposes provided it is necessary and proportionate);
  - Establish new Data Protection Commission; and
Agreements under GDPR

- Understanding the personal data that you are handling;
- Your role in relation to the personal data;
- Assessing roles and responsibilities;
- Data controller/Data Processor Contractual Relationships;
- Article 28 Data Processing Agreement;
- Managing Liability in Data Processing Agreements; and
- Other practical steps to consider.
What personal data will be processed in respect of day to day operations?


“business to business” personal data (“B2B Data”) – Product Producer to Service Provider – details of directors, secretary and designated persons of the Product Producer provided to Service Provider.

B2B Data – Service Provider to Product Producer – details of employees of Service provider provided to the Product Producer (e.g. point of contact / relationship manager of Service Provider).

“employee” personal data – respective personal data of employees/directors of Product Producer / Service Provider.
Your role in relation to the personal data

- In addressing and complying with GDPR you need to know in what capacity you are handling personal data –
  - Controller - determines purpose and means of processing i.e. what, when and how;
  - Processor - processes on behalf of the data controller; or
  - Both

- Product Producer (Fund, Insurer, Bank, Investment Firm) = Controller

- Service Provider = Processor when processing personal data on behalf of a Controller E.g. Fund (Controller) specifies what CDD is required from investors and Fund Administrator (Processor) processes that investor personal data on behalf of Fund.

- Service Provider = Controller in respect of personal data of own employees and in respect of performing CDD on own clients. E.g. Fund Administrator = Controller when performing CDD on Fund for its own AML purposes.
Product Producers will need to consider whether its appointed Service Providers are its Processors (i.e. processing data on its behalf) or whether they are Controllers in their own right.

A Service Provider may not automatically be a Processor on behalf of the Product Producer. Need to establish if Service Provider is using personal data for its own purposes?

The UK ICO Guidance on Controllers and Processors provides useful some guidance on this point:

- Degree of control Service Provider might have in respect of personal data;
- Decision making capabilities in respect of why and how of processing? i.e. why is it being collected, for what purpose and how it is held;
- Significant decision making.
<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Type of Data</th>
<th>Use of Data</th>
<th>Data Processor/Data Controller?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Investor Data</td>
<td>collecting and holding as part of share application process and AML compliance on behalf of the Fund</td>
<td>Data Processor</td>
</tr>
<tr>
<td>Administrator</td>
<td>B2B Data</td>
<td>uses information to satisfy its own AML requirements</td>
<td>Data Controller</td>
</tr>
<tr>
<td>Investment Manager</td>
<td>Investor Data</td>
<td>holds information to facilitate ongoing investor relationship management in respect of the fund</td>
<td>Data Processor</td>
</tr>
<tr>
<td>Investment Manager</td>
<td>B2B Data</td>
<td>uses to facilitate direct marketing of other funds on its own behalf</td>
<td>Data Controller</td>
</tr>
<tr>
<td>Depository **</td>
<td>B2B Data</td>
<td>uses data relating to individuals in the investment manager/administrator to perform obligations under the agreement</td>
<td>– Data Processor/Data Controller **  ** Divergent views in the market</td>
</tr>
</tbody>
</table>
Agreements between Product Producers and Service Providers should address role of each entity in respect of relevant personal data;

Where a Service Provider is “processing personal data” on behalf of Product Producer then a written contract is required which must comply with Article 28 (3) of GDPR – Data Processing Agreement;

Where dual use i.e. as Controller/Processor will need to address issues as to liability and indemnity;

If a Processor goes beyond what is agreed with the Controller in the Data Processing Agreement i.e. determines the “purpose and means” of processing, it will be treated as a Controller in respect of that processing: Article 28(10).

Agreements will need to reflect reality of operations.
A Controller may only use a Processor that will process personal data in accordance with GDPR and the processing must be governed by a written contract. Art 28(3) sets out nine requirements that must be present in this contract. These include:

(i) Only process personal data on documented instructions from the Controller;

(ii) Have appropriate confidentiality arrangements in place;

(iii) Take all organisational and technical measures required pursuant to Art 32; and

(iv) Assist the Controller in demonstrating compliance with GDPR, respond to requests for exercising data subject rights and assist the Controller in ensuring compliance with Articles 32 – 36.

Sub-Processing: a Processor may only engage a sub-processor if authorised to do so by the Controller. Where a sub-processor is engaged by a Processor, the same standards set out in the Controller/Processor contract must be set out in the Processor/sub-processor contract.
Controllers may seek to include an unlimited liability clause in Data Processing Agreements. For example – “in relation to any breach or potential breach regarding personal data processed by the Processor, the Processor’s liability shall be unlimited for each and every individual breach”.

Processors will want to limit and manage liability so may wish to include language in the Data Processing Agreement to manage such liability. Examples include –

Parties agree that the Processor shall not be liable for any Losses to the extent they are in respect of -

- Any processing by the Processor in accordance with the instructions of the Controller or

- Any breach by the Controller of Data Protection laws.
Other practical steps to consider

- Creation of a Register – To track Data Processing Agreements with Service Providers, which identify among other things the date signed, relationship manager, any specific requirements;

- Communication of “specific requirements” to employees – for example escalation of breaches / potential breaches;

- Creation of an audit process to review the implementation of Data Processing Agreements – for example questionnaire, on-site visit, compliance certification.
Any questions?
Contact

33 Sir John Rogerson’s Quay, Dublin 2, Ireland
Telephone +353 1 66 700 22
Fax +353 1 66 700 42

E-Mail: breeda.cunningham@dilloneustace.ie
Website: www.dilloneustace.com

Dublin    Cayman Islands    New York    Tokyo