Gem Briefing Note 18/1

March 2018

Purpose of this Briefing Note

The EU General Data Protection Regulation ('GDPR') (and associated E-Privacy Regulations and UK Data Protection Act) will be implemented in the UK from 25 May 2018. The GDPR will have the effect of replacing the existing UK Data Protection Act 1998 ('DPA 98').

This briefing note is intended as guidance to Gem clients on the GDPR including how to prepare for implementation. If not already doing so, firms should ensure that they have implementation plans in place and are progressing these in a timely manner before 25th May.

Introduction to GDPR

Many of the main concepts and principles of the existing DPA remain the same. However, there are many new elements and enhancements, some (but not all) of which are listed below:

- requirements apply to both data controllers and data processors;
- broader definitions of 'personal data' i.e. personal data will include IP addresses;
- increased controls on consent to obtaining and holding data including 'positive' opt in, not just implied;
- rights of data subjects improved including the right to be forgotten (subject to any other legal requirements on record keeping being complied with i.e. FCA);
- changes to subject access requests including that these will be free rather than a potential charge being levied;
- data breaches: increased responsibilities and procedures regarding reporting these to the Information Commissioner ('ICO').
- changes to ICO registration requirements for data controllers including changes to costs; and
- updated privacy notice requirements.

Please find below some high-level guidance from the ICO on initial steps in preparing for GDPR compliance.
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

What is Personal Data?

Personal data is defined as follows:

- 'Data' which relates to a living individual (the 'data subject') who can be identified from those data, or from the data and other information which is in the possession of, or is likely to be come into the possession of, the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

Guidance on who is a data controller or a data processor is shown below. Firms should also consider whether they are acting in both roles in different capacities according to their business model.

- A data controller means a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data processor is an entity which carries out processing on behalf of the data controller. Guidance on what constitutes 'processing' is also included in the Regulation and also on the ICO's website.

Who regulates this?

The Information Commissioner's Office ('ICO') is the UK Data Protection Regulator rather than the FCA and provides a good source of guidance on requirements. However, FCA requirements for firms systems and controls on data security also overlap with the ICO's and GDPR scope.

FCA rules at SYSC 4.1.5 include reference to data security and further guidance is also set out in the FCA's Financial Crime guidance book (Part 1) linked below. The FCA and ICO have also recently issued a joint statement on GDPR implementation.
https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr
https://www.handbook.fca.org.uk/handbook/document/fc/FC1_FCA_20160703.pdf (see Chapter 5 for Data Security).

Issues to consider include:

The step that firms are recommended to carry out include a 'data flow' identification exercise or audit. This is to enable the firm to identify:

- what personal data the firm holds;
- on which data subjects it holds it;
- what that data is used for, and subject to that, whether the firm has positive consent for this, and how/when that is obtained;
- where the data is stored;
- who, if anyone, is processing data on behalf of the firm;
- to whom data will be disclosed and how; and

- identifying if any of the data is ‘sensitive’ data as defined and if so, any additional protections that must be applied for that data.

If firms have not already commenced this exercise, we strongly recommend that this should happen as soon as possible. It is recommended that all relevant parts or stakeholders in the firm should be involved in this exercise.

This is not just an exercise for internal compliance or IT, as it is a business issue. Therefore, this should be led in the first instance by the management group and include for example HR (bearing in mind employee data) and the firm’s legal advisers (for client contractual documentation or disclosures).

Training

Firms should ensure that all staff in the firm, not just those involved in regulated activities, have received appropriate training on this well before May implementation.

Firms are encouraged to also identify, obtain or provide appropriate training especially for any staff who may be assigned formal Data Protection Officer responsibilities.

Data Protection Officer

For some UK firms, the need to formally appoint an individual with the title Data Protection Officer will be mandatory and further guidance on which type of firms this impacts on is also provided on the GDPR section on the ICO website.

We anticipate that a mandatory allocation of title will not be required. However ultimately that is up to each firm to determine.

However, in the same way that firms should have a clear allocation of responsibilities, we recommend that at the least responsibility for Data Protection is clearly assigned, (similar to Data Security/IT) which if not to an named individual, at Board/Management Group responsibility.

ICO Data Controllers Registration and Fees

Under current legislation, entities which are deemed to be data controllers are legally required to notify the ICO and to be added to the ICO register or otherwise this is a breach of current legislation unless an appropriate exemption applies.

Post GDPR implementation, it will not be a requirement to be on the register. However, all data controllers (as defined) will be required to pay an annual fee. The ICO has issued recent guidance on the fee requirements post GDPR and this is attached below.

It should be noted that until 25th May 2018, it remains a legal requirement for data controllers to be registered with the ICO. Therefore, any relevant renewals before that date should be continued unless advised otherwise by the ICO.

https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

Consent for Marketing Materials

Where firms issue communications externally including marketing materials to clients or investors, they should ensure that well in advance of GDPR, they can evidence that they have notified clients of the need of the firm to obtain positive consent to this prior to 25th May.

Otherwise the firm will no longer be able to issue such marketing materials.

Records should be maintained on positive consents received and if consent is not received by the implementation date, for mailing lists to be updated to take out any recipients who have not consented.

Commercial contracts

As part of contracts with clients – and suppliers - firms should also ensure that such terms and conditions include updated GDPR compliant Privacy Notices, which also have more prescriptive requirements in content. Again, further guidance on the ICO website is available on this.

Firms should liaise with their legal advisers as to any contractual documentation that should be updated and re-issued prior to May 2018.

Website and e-Privacy Regulations

To co-incide with GDPR implementation, updated E-Privacy Regulations are also being implemented at the same time which may impact on firm's websites.

We recommend that all firms should evidence an internal review of their website prior to May 2018, working alongside any IT resources required to do this. IT resources should also be familiar as to these requirements where this is provided by IT outsourced firms.

This includes that where required i.e. where personal data is collected via the website, that an up to date GDPR compliant Privacy Notice is disclosed on the firm's website. In addition, firms should bear in mind Cookies Consent and general guidance on this including that it should be clear and simple for website browsers to understand the firm's use of Cookies and either consent, or understand what affirmative action will be taken as consent, or refuse to their use when first accessing the website.

Next steps

As detailed above, this legislation relates to general EU and UK legislation for businesses and entities and does not directly or only relate to FCA financial services compliance.

If you have any specific questions on GDPR compliance, we suggest in the first instance that you refer this either to the firm's own legal advisers, IT providers or a GDPR specialist firm depending upon the nature of the query as described above.

However, if there is anything you need to discuss with Gem Compliance in the meantime or at any time including potential data security breaches either under current or future requirements, please contact us.