GDPR Blog Chapter One: – THE PLAYERS ON THE DATA PROTECTION STAGE

At the conclusion of our article on GDPR in last week's Bar Talk, we said that we would provide bite size chapters ("hereinafter "the Chapters") to assist you in understanding the new GDPR ***and update this when DPA 2018 arrived***. Welcome to Chapter 1 ***which has now been added to and modified by DPA 2018. When you see "GDPR" take this to mean "GDPR + DPA 2018" unless otherwise indicated.***

We thought it sensible to go back to basics. So, in Chapter 1 we will:

(a) set out the main concepts in data protection
(b) identify the main players on the data protection stage (including those under the GDPR).

(a) Data Protection Concepts

Everything revolves around "**personal data**" and how this is protected.

"Personal data" This includes information about (i) an already *identified* natural person and (ii) an *identifiable* natural person - that is, someone you can identify directly or indirectly from one or more characteristics (e.g. name, number, location data or more personal data such as a physical or genetic data).***The definitions are pretty much the same in the GDPR and DPA 2018 and can be found in full at Article 4(1) and sections 3(2) and 3(3) respectively.***

"Personal data" excludes information about deceased persons, corporate and similar entities. However, commercial clients would also expect that proper safeguards are taken to protect their data.

The whole aim of the GDPR is to control the way "personal data" is handled. As with the Data Protection Act 1998 (the DPA 1998), so with the GDPR; to fall within the GDPR, personal data has to be **"processed"**. That includes just about every conceivable thing you can do to personal data, from collection to storage, to adaptations and alterations, consultation and use, all the way through to its destruction. For the full explanation, please see the Bar Council's full guidance *[here].****The definitions are identical in GDPR and DPA 2018, for which see Article 4(2) and section 3(4) respectively.***

This is not limited to electronic processing – by laptop, tablet etc. "Processing" covers hardcopy files too – but, in order to qualify, these need to be in "a filing system" (GDPR Article 2(1) and Article 4 Definition ***and DPA 2018 section 3(7)***. Put simply,

can you get your hands easily on personal data because it is sensibly organised? For example, a corporate personnel department probably has a manual file for each employee and can easily locate individual personal data. The GDPR says the filing system is *"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".*

The key word is "structured". If personal data is scattered randomly around different ***manual*** files, these don't count. Why not? Simply because random bits of data are less likely to cause harm if released and, the effort of locating these is disproportionate to the likely resulting damage.

Just as an aside, and not because it affects you or your chambers, note that DPA 2018's definition of "processing" is made subject to other parts of DPA 2018 which make specific provision with regards to processing (Section 3(4)). The two main parts which you can ignore are Part 3 (Law Enforcement Processing – i.e. those bodies or individuals involved with crime and security work listed in Schedule 7) and Part 4 (Intelligence Services Processing i.e. GCHQ and Intelligence Services) - unless, of course, you are advising any of these bodies or individuals on their legal rights and obligations.

The DPA 1998 also identifies "**sensitive personal data".** What was sensitive personal data under the DPA 1998 is now called "Special Categories" under Art.9 GDPR. The definition is also somewhat plumper in its ambit. It is "personal data" that covers a person's: (i) racial or ethnic origin, (ii) political opinions, (iii) religious **or philosophical beliefs, (**iv) trade union membership, (v) physical or mental health or condition, **including the provision of healthcare services which reveal a person's health status,** (vi) sex life **or sexual orientation**, (vii) **processing of genetic and biometric data, to uniquely identify a person.** [GDPR additions in **bold**]. Data about criminal offences and convictions (previously included in sensitive personal data) are now dealt with separately, under Article 10.

It is worth spelling out "Special Categories" given the Bar's direct involvement with many of the areas covered. There are additional safeguards imposed by GDPR ***and DPA 2018*** in respect of processing this type of data. We will address these in another Chapter. ***Incidentally, there is no actual definition of "Special Categories" in DPA 2018. These are addressed in sections 10 and 11.***

Please note: "Criminal" is not in the Special Categories. Stricter requirements apply to personal data relating to criminal convictions and offences". ***We will provide a separate Chapter on this subject.***

(b) The key players on the GDPR and DPA 2018 stage

The Data Controller

The "**data controller**" is the natural or legal person ultimately responsible for determining the purposes for which personal data is processed and the means by which this happens.

In Bar terms, each individual practising barrister is a data controller if he or she is processing the personal data previously described.

Each set of chambers may also be a data controller for chambers management purposes. It may, for example, process personal data about employees and their appraisals, marketing activities, and payroll.

The ultimate compliance with GDPR (as with the DPA 1998) lies with that barrister or those chambers, respectively.

DPA 2018 modifies this to the extent permitted under GDPR Article 4(7). Essentially, where personal data are only processed for the purposes of an Act of Parliament and by means which are specified in the Act, the person who has the obligation to process the data becomes the data controller. (section 6(2)).

The Data Processor

Under the DPA 1998, it was the data controller who carried the can if something went wrong (DPA 1998 s.13). The data processor was merely an individual, or more likely a company, who (which) carried out processing work but had no say over the purposes for which this was done. Under the GDPR, the data processor has a bigger role to play and can be liable for its actions in certain circumstances.

Why do we even mention this? A barrister is certainly a data controller; he or she may also be a data processor. Why? It may be that you are carrying out work on behalf of chambers e.g. you are responsible for the administrative side of recruitment or you are involved in management committees.

Chambers may also be a data processor. Self-evidently, at the very least, it processes your work (within the general meaning of that word in the legislation) and saves it onto its own computers.

The Data Subject

It follows logically from our description of "personal data" above that this data must be about someone. That someone is the "**data subject",** one of the principal actors in data protection – and for your purposes, if it is an individual this could be your client (lay or professional) or their employees. The GDPR tries to shore up the privacy rights of the data subject by imposing a whole series of duties on data controllers. We will return to this theme in the Chapter 2.

The Information Commissioner

The DPA 1998 established the Information Commissioner (s.6): the regulator or Supervisory Authority for data protection in the UK. Under the GDPR, the Information Commissioner's Office continues in that role. ***This is acknowledged by the DPA 2018, under which the Information Commissioner continues in existence (Part 5, s. 114(1)), and continues to be the Supervisory Authority (s.116). See also Schedules 12 (the detail underpinning the position) and 20 (Part 6), (the transitional provisions between the DPA1998 and the DPA2018).***

Part 5 – s.115(2)- specifically incorporates the wide range of tasks, duties and powers of the Information Commissioner set out in GDPR Arts. 57 and 58 without restating them but at the same time qualifying them e.g. a certain function can only be carried out in accordance with a particular section of the DPA 2018 (for an example, see s.115(6)).

This section (s.115) also refers to the over-arching general duties imposed on the Information Commissioner in DPA 2018 s.2(2).

The Commissioner's mission is to promote good data protection practice by data controllers. He/she is accountable to Parliament. ***(see DPA 2018 s.139 and GDPR Art.59)*** He/she is responsible for promulgating codes of practice ***(see now the duty to do so under DPA 2018 s.121-128 and the scope of the presently envisaged codes)*** and general guidance concerning data protection practice. In respect of GDPR, the Information Commissioner has written a checklist document which provides a helpful tool to members of the Bar and sets of chambers**.**

The Information Commissioner is also the enforcement authority for data protection. He/she is responsible for investigating breaches of data protection practice and issuing enforcement notices and levying fines if these are justified – ***see Chapter 8 in this blog series***.

Under the DPA 1998, barristers and chambers may have done little more than register with the ICO. As a barrister, you may not have noticed this, as standard wording was available to cover the Bar's activities. You may not have even noticed the payment of the annual registration fee if this was arranged by your chambers. ***The DPA 2018 makes provision for data controllers to pay charges to the ICO (s.137, Schedule 20 para 26 and The Data Protection (Charges and Information) Regulations 2018 SI 2018/480) See the Bar Council's note on data protection fees here, and the ICO's guidance in relation to the fee.***

Conclusion

We have sought to explain some of the key terminology in data protection law and establish the cast of key players. Next week, we will deal with the players' rights and obligations. In particular, we will

(a) define their responsibilities under the DPA 1998
(b) show how these responsibilities have changed under the GDPR
(c) give examples of how issues can arise in daily practising or chambers life.

Bar Council IT Panel