GDPR Blog Chapter 6: The Data Processor – ***updated for the Data Protection Act 2018***

Welcome to Chapter 6. Over the past few weeks, we have dissected the General Data Protection Regulation (GDPR) which will be in force in the form of a new Data Protection Act hopefully by 25 May 2018. ***It is now in force as the DPA 2018.***

As we have previously recorded, in order to assist you, we have broken down the new Regulation into a number of scenes, dubbed Chapters. There is an Introduction (the Programme) *[here]*,Chapter 1, (the Players) *[here]*, Chapter 2 (Roles of Principal Members of the Cast – the Data Controller) *[here]*; Chapter 3 (A Continuation of the Data Controller's role) *[here]*; Chapter 4 (Further data protection principles with which the Data Controller has to comply) *[here]*, and Chapter 5 (Roles of Principal Members of the Cast – the Data Subject) *[here]*.

Chapter 6 looks at the third main member of the cast – the **Data Processor.** As barristers, your principal role will be as **Data Controllers**; i.e. it is you who decides what information about an individual you are going to process ("personal data", if you have forgotten the expression) and the purposes for which you are processing it. It is you who is responsible if that data goes missing or is the object of a cyberattack.

The role of a Data Processor has always been seen as the person (or organisation) which processes data for and on behalf of a Data Controller. The Data Processor really had no liability under the Data Protection Act 1998 if things went wrong. The GDPR changes this by imposing obligations directly on Data Processors.

You might ask, if I am a Data Controller, how can I be a Data Processor as well? The answer is that you may not be choosing the data or determining why you are processing it. It may be handed to you. So, you may be handling recruitment on behalf of chambers, or dealing with management committee issues discussing, for example, disciplinary action against an employee.

The same is true of chambers, or, depending on how chambers is organised, the Head of Chambers. They may act as Data Controllers for the data which *they* wish/need to process (e.g. pupillage, staff employment, external services), but they are also processing *your* data as Data Processors when e.g. they store it on a computer, such as an email server.

Art.28 is the principal Data Processor article in the Regulation – but reference is made in this to Articles 29-33. A lot of it concerns the Data Processor's obligations which almost certainly will be incorporated into standard contracts. Indeed, the EU Commission and the ICO are given the right to do just this – Arts.28(7) and (8).

What do these Articles mean for the Bar and Chambers?

- Data Controllers have a duty to select Data Processors who can meet the standards of the Regulation and ensure protection of the rights of Data Subjects. That is almost certainly not an issue internally between barrister and chambers, but remember that you/chambers may want to store data in the "cloud" or use external IT consultants to provide assistance to you. So, a certain amount of due diligence is required.

- If you are a Data Processor, you cannot engage another Data Processor without the specific agreement of, or general authorisation from, the relevant Data Controller (who can, of course, object).

- The Data Processor must also inform the Data Controller of intended changes (e.g. addition or replacement of sub-processors), again giving an opportunity to object.

- Subject to the above if a Data Processor (think: payroll provider) contracts with another Data Processor to carry out some or all of the processing work, the obligations of the original contract must be "passed through" to the new Data Processor. The new Data Processor must also take appropriate steps to comply with the Regulation. If the new Data Processor fails in its obligations, the initial Data Processor is fully liable to the Data Controller.

- There has to be a binding written contract or other legal act (such as a binding document formally adopted at a chambers meeting - which includes all the relevant terms set out below)) in place between Data Controller and Data Processor. "Written" includes "electronic". This has to specify (a) the subject matter being processed, (b) the duration of processing, (c) the nature and purpose of the processing, (d) the type of personal data, (e) the categories of data subject, (f) the Data Controller's rights and obligations.

- The contract has to have certain terms in it regarding the Data Controller's obligations. Summarised, these are:

  (a) data can only be processed on documented instructions especially as regards transfers to foreign countries;

  (b) confidentiality provisions;

  (c) suitable security measures are in place e.g. encryption and backup (see Art. 32 for the full list);

(d) express limitations on retaining another data processor (see second bullet point above);

(e) assisting the Data Controller with Data Subject access requests;

(f) assisting the Data Controller to comply with the implementation of security measures, notification of data breaches to the ICO and the Data Subject, impact assessments and consultations - you can read these in detail in Articles 32-36;

(g) deleting or returning personal data to the Data Controller at the end of processing e.g. when a barrister leaves chambers – Data Controller's choice as to which it is;

(h) deleting existing copies unless UK law requires them to be stored;

(i) demonstrating compliance with these obligations to the Data Controller.

- Pupils (other than pupils doing their own work), mini-pupils and devils will be acting as Data Processors. Contracts with between them and barristers (as Data Controllers) will also be required.

Record Keeping (Article 30)

Everyone keeps records these days – even Data Processors. If you (or Chambers) are acting in that capacity you have to keep records (in writing or electronic format) of the following. The extent to which these obligations will apply to barristers is not currently entirely clear. (See "Let outs to record keeping", below.) If the obligation does apply

The Data Controller has to keep the following information:

- Who is the Data Controller (and any representative, joint controller or Data Protection Officer)
- Contact details for the above
- The purposes of the processing
- The categories of data subjects and personal data
- The categories of recipients of the personal data e.g. courts, solicitors, regulatory bodies etc.
- Details of third countries (or international organisations) to which Personal Data is being sent
- The retention/erasure time limits set if possible

Details of security measures employed (see Article 32 for more detail).

The Data Processor (and any representative) has to keep the following information:

- Who is the Data Controller (and any representative, joint controller or Data Protection Officer)
- Any processors you are working for (and any representatives)
- Contact details for the above
- What categories of processing you are carrying out for each Data Controller
- Details of third countries (or international organisations) to which Personal Data is being sent
- Details of security measures employed (see Article 32 for more detail)

Let outs to Record Keeping?

The good news is that this record keeping does not apply to enterprises or organisations employing less than 250 people. But, before you breathe a sigh of relief, there are important exceptions to this general rule. They are where:

- The processing may result in a risk to the rights and freedoms of Data Subjects
- The processing is not occasional
- **The processing includes "special categories" of data** (i.e. in the old parlance under the Act, "sensitive data" ; see *[here]* to remind yourselves of what this is)
- The processing relates to criminal convictions and offences

  The reference to processing being no more than "occasional" could be problematic - if it is read too literally the exemption would apply to very few enterprises or organisations.

If the obligation to keep records does not exist you may In any event wish to keep those records anyway. You may also find it useful to keep the following records:

- adoption and implementation of a data retention policy – this will require a copy of the policy itself, and a record of the date of its adoption;

- the dates on which personal data is reviewed and deleted, and the reasons for deciding to retain personal data after the initial retention period;
- a copy of all privacy notices and a record of their review dates;
- the reason for deciding not to provide a data protection notification under Art. 14;
- confirmation of the secure disposal of a hard disk drive or other storage device containing data, and the method of disposal used;
- participation in information security training - depending on your CPD plan this may count towards your CPD.
- records of any breach and the steps taken in mitigation.

Some firms have solicitors have asked barristers to sign agreements which impose on barristers the obligations which apply to data processors. In an ordinary barrister/solicitor relationship it would be inappropriate for a barrister to sign such an agreement as the barrister is a data controller and not a data processor. For further guidance on this point see https://www.barcouncilethics.co.uk/documents/signing-controller-processor-agreements-with-solicitors-firms/.

Final Note: If a Data Processor assumes the mantle of a Data Controller and thereby infringes the Regulation – i.e. the Data Processor determines purposes and means of processing – that Data Processor will be considered as a Data Controller.

The DPA 2018 does not change the position regarding the data controller/processor relationship as set out in the GDPR.

Bar Council IT Panel