GDPR – THE ROLE OF A DATA CONTROLLER /cont.

Welcome to Chapter 3. A brief update for those who have missed our words of wisdom so far. There is a new play about to hit town in May 2018. Sitting somewhere on the Aristotelian theatrical scale between a comedy and a farce, with plenty of melodrama (for those who get it wrong) and a smattering of history, the overall production is markedly more interesting than watching paint dry.

The Europeans have invented a new Data Protection regime. It is far more comprehensive than the previous regime and places more duties on the Bar and chambers than ever before.

In order to assist you, we have broken down the data protection play 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) *[here]*.You cannot really follow the plot, unless you read these – so please do. Seriously, it could save you a lot of anguish in the long run.

This Chapter 3 finishes off (no, not kills off; that is reserved for the theatre!) the data controller's role with regards to Principle 1. See the Bar Council Guidance for more information on the points covered.

Chapter 2 concluded with a look at the **first data protection principle**, namely that data should be processed "lawfully, fairly and transparently" - or rather, one third of it as space precluded a look at the words "fairly and transparently". We will remedy that situation now.

Fairness

"Fairness" can be dealt with relatively quickly. It is not believed that the GDPR changed the meaning of fairness under the Act, which includes holding a balance between the data subject and the data controller. ***Likewise, the DPA 2018 does not change matters.***

Transparency

What does "transparency" mean? In a nutshell, "openness about who you are and what you are doing in your dealings with your clients and others".

You need to look at GDPR Arts 12-14. These cover the situations where (1) you collect data relating to that data subject from him or her (Art.13), and; (2) you receive personal data that has not been obtained from a data subject (Art.14). Actually, the requirements in each Article are very similar, but before you breathe a sigh of relief, they are very detailed.

In addition to the requirement to notify, other major points to note are the requirement to notify the legal basis for processing, including the nature of legitimate interests which you rely on, and the period for which you will be keeping the data – see below.

What do these Articles mean for the Bar and Chambers?

1. Where you or your Chambers obtain data relating to a data subject from that data subject (e.g. a client, a witness, a pupillage applicant, a prospective employee), you have to give that person certain details about who you are and what you are doing with their personal data – ***this is subject to the exceptions referred to below***. These ***details*** are:

- Your identity and contact details
- If you have a representative or data protection officer, their contact details (unlikely to arise for the Bar but listed for completeness)
- The purposes for which you are processing any data (e.g. to provide legal advice or draft a particulars of claim)
- The legal basis for processing the data (e.g. most obviously "to enable me to provide legal services". Less obviously e.g. "for fee disputes" – see Guidance)
- The categories of personal data involved (Article 14 only – fairly obviously as if they are giving you the information, they know what they are handing over)
- If you are processing data in pursuance of your own legitimate interests, (or a third party's) - Art 6.1(f) - what those interests are. You will have considered and recorded these when preparing your Data Protection Policy.
- Details of who is going to receive any of the client personal data – e.g. my solicitor etc - or categories of these persons – e.g. the probation service, the courts etc – see the GDPR Guide for a fuller list.
- Details of likely transfers of personal data if any, to a third country or international organisation – please see Art.13.1 (f) for the full requirements
- How long you will store any personal data, or, if you cannot determine the actual time, the criteria used to determine the period. You will have considered data retention periods when preparing your Data Protection Policy, and you will need to notify data subjects of the retention period which you adopt
- The rights the client has: for access to his or her personal data, rectifying inaccuracies, deletion of personal data, restrictions on processing and the right to port that data to another data controller (these will probably become standardised words)
- The right of the data subject to withdraw consent to your continued processing of personal data (i.e. the opposite of Art 6.1(a) and Art.9.2 under which consent is explicitly given)
- The right to lodge a complaint with the Information Commissioner's Office (again, standard words will cover this)

- Whether the provision of personal data to the barrister arises from a statutory requirement or a contractual one (or a requirement necessary to enter into a contract). In the case of the Bar, it is likely to be contractual.
- Whether the client is obliged to provide his/her personal data and the consequences of failure to do this (e.g. you cannot do the work)

2. As we have said, Art.14 requirements are similar to those in Art.13. Notable additions in the latter case are that (a) you have to give details of where the data originated from and if it came from publicly accessible sources; (b) the information has to be given to the data subject within a reasonable time after receipt and at the latest within one month from receipt; (c) if the personal data are to be used for communication with the data subject, then details have to be given at the first communication with that person; (d) if disclosure to another recipient is anticipated, then the information is to be provided at the latest when the personal data are first disclosed.

The DPA 2018 has something to say about these sections - see s.15 and Schedules 2, 3 and 4. Yes, sorry, we are back to Schedules. The right to restrict the ambit of these arises from several GDPR Arts. - 6(3), 23(1), 85(2) and 89(2). We mentioned at the start of these blogs that the GDPR allowed Member States to adjust rights and obligations in some of the GDPR Articles.

Keeping this as brief as we can,

- ***the obligation on you as a data controller to supply the detailed information set out above (either under Art.13 or 14) when you collect personal data for processing does NOT apply in respect of cases of (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders, (c) assessment or collection of taxes, to the extent that provision of any information could prejudice any of these matters. (Schedule 2 para 2)***

- ***if, as the first data controller, you have to hand over this personal data to a second controller (e.g. for the second controller to carry out functions required by statute), then the second controller is exempt to the same extent as the first (Schedule 2 para 2)***

- ***in both of the foregoing, you are also not obligated to tell a data subject of any personal data breach e.g. you have lost his or her data. Normally you are required to tell a data subject about a data breach – see GDPR Articles 34(1) and (4). (Schedule 2 para 2)***

- ***Art.13 and 14 also do not apply to personal data where disclosure of the data is necessary (a) for the purpose of, or in connection with, actual or prospective legal proceedings, (b) obtaining legal advice, or (c) is otherwise necessary to establish, exercise or defend legal rights, to the extent that applying Arts. 13 or 14 would prevent the data controller from making the disclosure. Is this significant for the day-to-day practice of a barrister – except for (a) above probably not as the text refers to a data controller disclosing rather than receiving and processing the personal data. However, a quick reading might have suggested otherwise, so we include it here. (Schedule 2 para 5)***

- ***Art.13 and 14 also do not apply where an order of the Court or a tribunal requires that disclosure should be made, to the extent that the application of those provisions prevents you as a controller from making the disclosure (Schedule 2 para 5)***

- ***Arts. 13 and 14 do not apply AT ALL to personal data processed by you if you are working in a judicial capacity (Schedule 2 Part 2 para 14(2))***

- ***Arts.13 and 14 do not apply AT ALL to personal data that consists of information in respect of which a claim for legal professional privilege could be made nor information in respect of which a duty of confidentiality is owed by you to a client (Schedule 2 Part 4 para 19). Art.14.5(d) itself states that Art.14 does not apply where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.***

3. In the event that further processing of client data for a different purpose arises, you also have to tell the client what that different purpose is, together with any further relevant information arising under 1 above. Plainly, if you are relying on consent, the original consent will not operate in relation to an undisclosed purpose. So, you cannot assume that one consent covers all.

4. Note: if the client already has any of the information above, you are not obliged to give it to him/her again (Art. 13). As Art. 14 concerns the situation where personal data have not been obtained from the data subject, there are one or two more exceptions to the requirement to provide information. Essentially these are:

    - The impossibility of providing information
    - Disproportionate effort in providing information
    - The provision of the required information renders impossible or seriously impairs the achievement of the objectives of that processing

- Obtaining/disclosure is already laid down in EU/UK law and contains appropriate measures to protect a data subject's legitimate interests
- Where personal data must remain confidential subject to an obligation of professional secrecy regulated by EU/UK law including statutory obligations of secrecy, for example the Bar Code of Conduct duty of confidence and legal professional privilege. ***For the first three of the above exceptions it may be necessary to make privacy information publicly available.***

5. It is likely that the proposed new Data Protection Act will contain additional exceptions and we will report on these in a final round up of changes. ***We have discussed these above.***

6. Sorry. You cannot charge for providing all this information. It is free. (Art.12.5). The only exception is that where requests are unfounded or excessive e.g. repetitious, a data controller can either charge a reasonable fee or refuse to act on the request. The burden of proof is on the data controller to show that requests were unfounded or excessive. ***Note that under DPA 2018 s.12, the Government may limit fees that can be charged in respect of unfounded or excessive requests.***

7. There are mandates for the manner in which you provide the information under these Articles. The information has to be concise, transparent, intelligible, and easily accessible, and use clear and plain language – especially when dealing with children. Family and Criminal Law barristers please note. The information has to be provided in writing, including electronic means. It can be provided orally if the data subject requests, providing that the identity of the data subject is proved.

8. You will therefore have to look at your privacy notices to make sure that these are up to date with GDPR requirements. These will be needed in respect of:

    - Clients, including direct access clients
    - Public – on chambers' website and/or barrister's own website
    - Candidates – for tenancy, pupillage or mini pupillage
    - Job Applicants.
    - Users of chambers or a barrister's own website

    Consultants have been engaged to prepare templates which will assist you.

    Further guidance is to be found at

    - ***the Bar Council's FAQ guidance at https://www.barcouncilethics.co.uk/wp-content/uploads/2018/12/GDPR-Frequently-Asked-Questions.pdf (Questions 1 to 10)***

- ***the ICO's updated guidance at*** ***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/****, and***

- ***the ICO's more detailed guidan***ce at ***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/when-should-we-provide-privacy-information-to-individuals/***.

Here are some examples of when you will need to consider notifying data subjects when working on a case:

1 When you are first instructed, you will need to notify the client. Subject to LPP and your duty of confidence, you may also need to notify persons closely connected with the client that you will be receiving their personal data, e.g. family members and employees of a company.

2 When you obtain personal data relating to third parties, you may be able to rely on the duty of confidence/LPP exception. But there will often come a time when you can no longer do so, e.g. after a document (such as a witness statement) has been read in court. Subject to what the new Act may say on this point, you may need to notify. You may also be able to rely on the "disproportionate" exception, e.g. if the solicitor has already notified the data subject or if you don't have contact details for the data subject.

3 If you take a witness statement yourself in a public access case, you will need to notify the witness setting out the matters we have addressed above.

In addition, you or your Chambers will need to notify other data subjects such as pupils and prospective employees.

If all of this has brought you out in a cold sweat, don't panic. The GDPR has to be all things to all men and women. Extensive work is being carried out to help you achieve compliance. However, you should be aware that this is likely to involve more thinking about your processes to get it right. The Riliance system will have additional guidance, draft policies and step by step guides for you to assess your compliance.

Next time

So much for the "**data controller"** and the First Principle. In Chapter 4, we look at the remaining Principles.

Bar Council IT Panel