GDPR Blog Chapter 5 – The Data Subject – *updated for Data Protection Act 2018*

Welcome to Chapter 5. After an Introduction and four previous Chapters, you should be right up there with the buzz about the new Data Protection "play" hitting town in May 2018. Based on a Regulation promulgated by that well-known theatre group, the Europeans, it is far more comprehensive than the previous regime and places more duties on the Bar and chambers than ever before. ***And, if you have been reading the previous blogs (you have been reading them haven't you?), you will know that there is a new Data Protection Act 2018 (DPA 2018) that incorporates the GDPR for the majority of processing activity.***

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]*; and Chapter 4 (Further data protection principles with which the Data Controller has to comply) *[here]*.

Why does the data controller merit three Chapters? Because that person is either you or your chambers. It is important therefore to know what you have to do when the Regulation rolls into town. Actually, it will roll in as a new statute. This has been published as a Bill and there is lobbying and review going on at the moment. Since it is likely to change, we won't trouble you with the Bill. We will provide an update later on when this becomes law ***which, as we have said, it has now, as DPA 2018.***

Chapter 5 looks at the other side of the coin – the **data subject** aka (in most cases) your client, but may be anyone. You are required to give data subjects the information that we set out in Chapter 3. However, that does not stop them coming back some time later, after the case has finished, and asking what it is about them that you are processing.

What rights does such a data subject have, viewed from that person's perspective? These are set out in Chapter III of the Regulation. They consist of the following main topics.

Transparency

Chapter 3 described your obligations to provide information to data subjects and this has to be done in concise, transparent, intelligible and easily accessible form, particularly where children are concerned – see Art.12. Information is to be supplied

free of charge. To the extent that we have discussed this area previously (with reference to Arts.13 and 14), there is no need to repeat it here.

Subject Access Requests (Art.15)

Data subjects have a right to know whether or not you are processing their personal data. If you are doing so, they have a right of access to this and to some specific information from you. They also have a right to a copy of this, in writing or by other means, including where appropriate by electronic means. If the request is by email, then you are to respond by email unless the data subject otherwise requests. ***Given our remarks in the Introduction, it would be sensible to verify that the person sending the email is actually the person who wants his or her information and not some fraudster sending a spoof email; perhaps best to ask for a copy of some identification document to be produced to you.***

You must provide information on action taken on requests under Art.15 (and incidentally Arts. 16-22- see later) without undue delay and in any event within one month of receipt of the request ***(once you have verified that you really are dealing with the real data subject)***. This can be extended by two further months where necessary (taking into account the complexity and number of requests), but you need to tell the data subject – see Art.12(3)).

Judging by the text, the first copy is free; later copies attract an administrative fee. You only have to know this if someone makes a request. Otherwise, you can park it in the back of your minds for the moment. The information required is:

- Are you actually processing that person's personal data?
- The purposes for which the data is being processed
- What categories of data are you processing?
- Who (specifically or by category) is receiving this data, in particular, where those recipients are located abroad (and if located abroad, what safeguards were adopted (for which see our later Chapter on transferring data abroad)
- How long will you be storing the data, or if you don't know, what criteria are you using to determine this period – your or your chambers Data Retention Policy should help you answer this question.
- The existence of the rights, to request correction or deletion of personal data, restrict the processing of data or object to processing at all
- The right to lodge a complaint with the Information Commissioner's Office
- Where you got the data from, if not from the data subject himself/herself.

The DPA 2018 says something about Article 15 in the form of an Art.23 restriction (see DPA 2018 Schedule 2 Part 3 para 16).

Art.23 restrictions are permitted provisions which the UK Government can introduce to restrict obligations and rights assumed by data controllers or processors in the situations enumerated in Article 23 (e.g. national security).

So far as Art.15 is concerned, you are not obliged as a data controller to disclose the information set out above to a data subject if to do so would involve disclosing "information relating to another individual" who can be identified from the information EVEN IF that other individual has consented to the disclosure or it is reasonable to disclose the information without consent.

If you consider it reasonable to disclose the information without consent, you have to take into account relevant surrounding circumstances. These include the considerations set out DPA 2018 Schedule 2 Part 3 para 16(3) e.g. any duty of confidentiality owed to the other individual.

"Information relating to another individual" includes

(a) information identifying that other individual as the source of information

(b) if that individual can be identified either from the specific information or that information and any other information that you reasonably believe that the data subject is likely to have or be able to obtain.

In addition, as a data controller, you are not required to divulge personal data that consists of information in respect of which a claim to legal professional privilege could be maintained, or information in respect of which a duty of confidentiality is owed by you to a client. (DPA 2018 Schedule 2 Part 4 para 19) OR you are sitting in a judicial capacity (DPA 2018 Schedule 2 Part 2 para 14).

Your Article 15 responsibilities also do not apply

- *to personal data you have processed for (a) the prevention or detection of crime, (b) apprehending or prosecuting offenders, (c) the assessment or collection of taxes or duties to the extent that your processing prejudices any of the foregoing (Schedule 2 Part 1 para 2)*

- *to any personal data where disclosure is required by a court or tribunal order, to the extent that this would prevent you from making the disclosure (Schedule 2 Part 1 para 5)*

- ***where disclosure of personal data is necessary for the purposes of, or in connection with, legal proceedings OR is necessary for the purpose of obtaining legal advice OR is otherwise necessary for the purposes of establishing, exercising or defending legal rights, to the extent that the application of the Art.15 provisions would prevent you from making the disclosure. (DPA 2018 Schedule 2 Part 1 para 5).***

That said, it would be unusual for any of the above three exceptions to be relevant to a subject access request made to a barrister in relation to personal data obtained in the ordinary course of a barrister's practice.

Rectification of data (Art.16)

This covers two angles.

Firstly, if personal data you are holding is inaccurate, you are obliged to correct this upon request.

Secondly, having regard to the type of processing you are carrying out, a data subject can request incomplete data to be completed.

As regards the DPA2018, the last three additional exemptions listed under Art.15 above apply, with of course, the necessary adaptations. For guidance from the ICO on the Articles to which particular exemptions apply see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/, or refer to DPA 2018 Schedule 2 itself. (In addition, www.gdpr-dpa.co.uk shows which exemptions apply to particular Articles.)

The right to be forgotten or erasure of data (Art.17 with reference to Arts. 6 and 21)

You may remember that this one caused quite a stir when it was first mooted a year or two ago. This concerned Google and others being requested to remove people's data where those people preferred others to forget inconvenient truths about themselves. Why should those with something to hide have their data deleted? This is the first time that there is statutory authority for erasure.

You have an obligation to do this, if so requested, and without delay, **but only in the following circumstances:**

- You have no need to hold onto the data any longer for the purposes for which you obtained it originally

- Consent to process is withdrawn by the data subject and there is no other legal ground for processing
- The data subject objects to the processing. He/she can do this (a) in the case of direct marketing – chambers managers watch out! (b) where processing is necessary for a task carried out in the public interest or in the exercise of official authority **unless** you can show that there are compelling legitimate grounds for continuing with the processing which override the data subject's interests, rights and freedoms or for the establishment exercise or defence of legal claims (c) processing is necessary for your legitimate interests as a data controller except where the data subjects interests, rights and freedoms override this (especially in the case of children)
- The personal data have been unlawfully processed
- The personal data have to be deleted to comply with a legal obligation in UK/Member State law

Life then gets a little complex. This probably won't affect you as barristers, but we will include it for completeness (and just in case you are affected). If you have made public any personal data, and a data subject has requested its deletion, you are bound to take **reasonable steps** (i.e. technology, how much it would cost to do this) to inform other relevant data controllers. If this ever happens to you – see Art.17.2.

Lastly, everything that we have just said, does not apply at all to the extent that processing is necessary:

- Where rights of freedom and expression are being exercised
- For compliance by you with a European or UK legal obligation, the performance of a task carried out in the public interest, or the exercise of official authority vested in you as controller. This would appear to be the obverse of the third bullet point above
- For public health reasons (as contemplated by Art.9(2) and 9(3))
- In respect of archiving in the public interest, scientific or historical research purposes or statistical purposes and deleting data would make this impossible or more difficult
- **For the establishment, exercise or defence of legal claims.**

So, after a detailed exposition of the right to be forgotten, it is likely that the Bar would ***in many cases be able to*** claim exemption from having to delete ***personal data*** under the final rubric in bold***, so long as the personal data still needs to be retained for the establishment, exercise or defence of legal claims. The data does need to be erased in accordance with Art.17 if it is no longer required in relation to a legal claim (eg where the data is of little or no significance), and the "legal claims"***

exception may not apply to personal data obtained in relation to non-contentious work which does not involve a "claim".

In the DPA 2018, some of the same additional exemptions apply to this provision as applied to Art.15 – see above.

Right to restriction on processing (Art.18)

These are the data subject's rights to ***restrict*** any processing you may be carrying out. They arise:

- Where the data subject alleges that data about him/her are inaccurate. The restriction is only for the period necessary for you to validate the accuracy of the data.
- The processing you are carrying out is unlawful but the data subject wants your use to be restricted rather than for the data to be deleted.
- You no longer need the data for the purposes for which they are being processed, but the data subject does need them for the purposes of establishing, exercising or defending legal claims.
- The data subject has objected to the processing taking place for one of the reasons set out in Art.21(1) - but the restriction of processing only applies for the time it takes to verify that your interests in continuing to process the data override the data subject's interests in seeking to restrict the processing .

What are the Art.21 reasons? In short summary, they are:

- You claim that you are processing information in furtherance of a task carried out in the public interest and the data subject disagrees
- You (or a third party) claim that you have legitimate interests in processing the data and the data subject claims that his or her rights and freedoms are more important.

In the event of any such valid restriction for the reasons set out above you can only process the data

- for storage purposes (without any consent being required), or
- with the data subject's consent, or
- in order to **establish, exercise or defend** legal claims, or
- in order to protect rights of another natural or legal person, or
- for public interest reasons.

Once you have overcome the various hurdles outlined, you have to tell the data subject that you will continue the processing.

Once again, the DPA 2018 applies a similar regime to that which we set out above under Article 15.

Data portability (Art.20)

The take-away data section! This applies only to electronically processed data not to any form of manually prepared file. The data subject has three rights:

- To receive the personal data about him or her that you have been processing
- To transmit this data to another data controller without interference from you
- To have the data transmitted to another data controller directly (if it is technically feasible to do so).

The data has to be presented in a "structured, commonly used and machine-readable format".

However, a data subject can only ask for this data on limited bases. These are:

- The processing was originally based on the data subject consenting to this.
- The processing was based on performance of a contract to which the data subject was a party or one which the data subject wanted to enter into.
- The right to receive personal data in the way described does not affect the rights and freedoms of others (i.e. you would have to redact details of other data subjects).

Once again, similar principles apply as for Art.15 above

The Right to Object (Art.21)

Article 18 set out the data subject's right to ***restrict*** continued processing. Art.21 allows an outright ***objection*** to the continuation of processing. Any objections must relate to that data subject's own situation, can be made at any time and must be based on either:

- You claim that you are processing information in furtherance of a task carried out in the public interest and the data subject disagrees.

- You (or a third party) claim that you have legitimate interests in processing the data and the data subject claims that his or her rights and freedoms are more important.

In the event of a complete objection from a data subject, you can only process his/her data

- if you can demonstrate compelling legitimate grounds for continuing with the processing which are sufficient to override the rights, interests and freedoms of the data subject, **or**
- **for the establishment, exercise or defence of legal claims.**

In many cases barristers may be able to rely on the highlighted exception in the event of an objection being raised, but please note the conditions under which this is available.

For chambers, a data subject has a right at any time to object to his/her data being used for direct marketing purposes. In such a case chambers must stop using such data.

Once again, much of the DPA 2018 regime we set out under Article 15 applies equally to this Article.

GDPR Chapter VIII – Remedies, Liability and Penalties

No discourse on Data Subject rights would be complete without mentioning Chapter VIII of the Regulation. We will simply mention these, as there is no action required of you unless you are the subject of a complaint or a claim for compensation. This Chapter sets out a series of rights. These are:

- The right of the data subject to lodge a complaint with the ICO if he or she believes the processing of his or her data infringes the GDPR together with the duty on the ICO to keep the complainant informed of the progress and outcome of the complaint (Art.77). ***The DPA 2018 s.165 contains additional provisions relating to this right.***

- The right to an effective judicial remedy against a legally binding decision of the ICO, or where the ICO does not handle a complaint or does not inform the data subject of the progress or outcome of the complaint (Art.78). ***This is now encapsulated in DPA2018 s.166. Reference is to the First Tier Tribunal or if Tribunal Procedure Rules so provide, to the Upper Tribunal (see DPA 2018 s.205).***

- The right to an effective judicial remedy against data controllers or data processors (Art.79) ***The issue of Court remedies to ensure compliance with***

data protection legislation is set out in DPA 2018 s.167, with s.168 containing additional provisions relating to GDPR Art.82 (the right to compensation).

- The right to compensation and liability (Art.79 ***should be Art. 82 – apologies to all who were misled.***). We will give this its own Chapter later on, together with the right of the ICO to issue fines.

Can the UK override any of these data subject rights? (Art.23)

This is one area where the UK can make its own mark. Data subject rights can be restricted by UK law in a number of instances. These are:

- National security
- Defence
- Public security
- Prevention, detection, investigation or prosecution of criminal offences or carrying out criminal penalties
- Other important objectives of general public interest (e.g. public health, social security)
- Protection of judicial independence and judicial proceedings
- Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- Monitoring, inspection or regulatory functions connected to the above (other than judicial proceedings)
- Protection of the data subject or the rights and freedoms of others
- Enforcement of civil law claims

The Regulation requires that any restrictions contain certain specific provisions – e.g. the scope of the restrictions introduced. We will not dwell on these here but rather report on them when the new Data Protection Act becomes law – ***which we have now done and these are reflected in the text above***.

Next time

We are still looking at members of the cast of this play. Next time it is "**data processors"** and the parts they play. Please read on in two weeks' time. It is more exciting than dealing with your credit card bills from Christmas or your tax return.

Bar Council IT Panel