GDPR Blog Chapter 2: THE ROLES OF EACH PRINCIPAL MEMBER OF THE CAST

Updated for the Data Protection Act 2018

Welcome to GDPR Chapter 2. We hope you found Chapter 1 informative.

For those who have missed the plot so far, let us offer you a catch-up. Much like any good stage play, (or come to that, book or film) you need to view the opening scenes rather than going straight to the middle or the end.

Please look at the Introduction *[here]* and Chapter 1 *[here]*. ***"Introduction" now has an Introduction to the Introduction" and both were published together in December 2018. In every subsequent chapter we will simply refer to the Introduction as covering both of these documents.*** The underlying plot is that there is a new Data Protection regime being introduced into the UK in May 2018. It is known as the General Data Protection Regulation (GDPR) and it goes further than ever before in seeking to protect an individual's personal information from unauthorised disclosure. In doing so, it places more onerous duties both on barristers and chambers. As we explained in the Introduction, you must be aware of these duties and act on them when the GDPR comes into force in May 2018. There are significant potential adverse consequences for not doing so. It could take just one Chambers colleague clicking on a link in a phishing email for all your emails on the Chambers server to be leaked to an intruder. ***As we have said in earlier blogs, the GDPR is now in force through the DPA 2018.***

We need to explain what all this means in practice. The Bar Council's IT Panel has decided to go back to basics and set out data protection and what you need to do about it, in simple terms. There is more detailed guidance available *[here]*.

The Introduction amounted to a programme for the play. It set the scene – what is the GDPR, why, in the context of today's world, it is so important and what could happen if it all goes wrong. Chapter 1 introduced the main members of the cast in the play.

In Chapter 2, we start to concentrate on the roles each member of the cast performs. Therefore, we will:

(a) Define the rights and/or obligations of each actor under the DPA 1998

(b) Show how these have changed under the GDPR ***and the extent to which the DPA 2018 has made modifications***

(c) Gives examples of how issues can arise in daily practise or chambers life and what to do about them.

The lead members of the cast are the "**data controller**" and the "**data subject**". The former decides what personal information about an individual is collected and "**processed**" - a very wide-ranging term; see *[here]* for the full definition. He/she is principally liable if things go wrong. The latter is the individual person whose personal information is processed by the data controller.

This time we will deal with **data controllers** – yourselves and your chambers. Note that you may both be **data processors** as well. We will cover that role in a later Chapter.

There is a lot that should be said about **data controllers** so that you know what to do. We will continue this subject in Chapter 3.

In Chapter 4 we will look at the extensive rights accorded to **data subjects.**

Data Controllers

The Principles

The DPA 1998 obliges a data controller to comply with a number of principles when processing personal data – s.4(1) and Schedule 1. Ignoring the bold type for a minute, there are 8 principles. In summary, these are:

(1) Personal data has to be processed fairly and lawfully **and in a transparent manner ("lawfulness, fairness and transparency")**

(2) This data can only be obtained (**collected)** for specified **explicit** and lawful purpose(s). It cannot be further processed in any way incompatible with these purpose(s) **except that further processing for archiving in the public interest, scientific or historical research purposes or statistical purposes does not amount to incompatibility ("purpose limitation")**

(3) Personal data is to be "adequate, relevant and not excessive"(**limited -note the change of emphasis; the minimum possible)** having regard to the purposes for which it has been obtained (**"data minimisation")**

(4) Data has to be accurate and kept up to date **and inaccurate data have to be erased or rectified without delay ("accuracy")**

(5) Data is not to be kept **in a form which permits identification of data subjects** any longer than necessary for the purposes for which it is processed **(and may be stored for longer in respect of the same research**

and archiving exceptions as in (ii) above, providing a data subjects rights are protected) ("storage limitation")

(6) **[**All data has to be processed in accordance with the rights of the data subject**]**

(7) Appropriate technical and organisational measures are to be taken against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, personal data **("integrity and confidentiality")**

(8) **[**Data must not be transferred to any country outside the EEA unless that country has adequate data protection provisions.**]**

The GDPR Art. 5 has updated these principles – and rescued them from obscurity in a Schedule in the DPA 1998. The changes are in bold letters above. In the GDPR, each principle has been given "a title". These are set out in bold and in inverted commas. Principle 6 is now used throughout the GDPR and does not need a separate place at the Principles' table. Principle 8 – transfer of data abroad has been removed – hence the square brackets. It now has its own chapter in the Regulation (Ch.5). A later Chapter will deal with this aspect.

A new responsibility

From a barrister and chambers point of view, there is a new explicit requirement in the GDPR attached to these principles. It is worth stating boldly: - **the Controller shall be responsible for, and <u>be able to demonstrate compliance</u> with the principles set out above – ("accountability") (Art 5(2)).** Previously under the DPA 1998, you merely needed to comply with the principles.

It is worth pausing at this point. The last sentence does not live in a vacuum. It is amplified in Art.24.

The gist of Art. 24 is:

(i) Appropriate "technical and organisational" measures <u>must</u> be implemented by a controller to ensure that processing is carried out in accordance with the Regulation.

(ii) These measures have to be reviewed and updated where necessary.

(iii) Implementation of the measures is variable and proportionate, and depends on the nature, scope, context and purposes of the processing against the risks to a data subject's rights and freedoms. Those dealing with patent work might be rather less at risk than family lawyers.

(iv) Where it is proportionate in relation to processing activities, a controller must implement appropriate data protection policies.

(v) In the future, compliance with Codes of Conduct and Certification Schemes will also assist in demonstrating compliance, but none currently exist so we can park this aspect for the moment.

What does this mean for the Bar and Chambers?

What does this actually mean in practical terms for the Bar and chambers? We would suggest the following:

- Re-read the Principles above and in the light of the expansion of these below and in the next Chapter, ask yourself if you can truthfully say you are complying with them. It is unlikely that you are as there are new obligations and extended existing obligations.
- Every barrister and Chambers will need to produce new policies addressing their data processing. There will be pro forma policies available in the Riliance system which will shortly be made available to barristers for 12 months. You will need to adapt these to your circumstances. If you feel incapable of doing this you can pay Riliance or another provider to do it for you.
- All decisions you make concerning compliance should also be recorded so that you can demonstrate your compliance if asked.
- Every barrister must comply with the data protection policy.
- This policy will include sections on how long barristers intend to keep personal data ("data retention") which may vary with different practice requirements. In some chambers you may all agree on e.g. retention periods, and be able to use common policies. If, however, you make different decisions about e.g retention periods, you will need your own policy. It is important that each requirement is listed, together with brief reasons why a particular period has been selected. This is one of the main "organisational" issues that catches people out – too much data is held onto for no reason. Of course, there are good reasons for keeping some data, for example for the purpose of possible complaints and for conflict checking. However, the data retained should be the minimum required for that purpose.

- Personal data will be in emails and files. Each barrister has to decide how long emails and files are to be kept. We will deal with data retention in another Chapter.

- "Technical" measures include implementing all updates, password implementation advice, encryption software that you believe are necessary (and if you have one your IT Manager may assist) in order to ensure the personal data is as secure as possible.

The Principles – a little more detail.

Many of the principles are self-evident in what they mean and how they might be put into practice. However, we do need to focus a little on the <u>first principle</u>.

Principle 1 – Lawfulness, fairness and transparency

Under the DPA 1998, "personal data" were <u>not</u> considered to have been processed "fairly and lawfully" unless one of the conditions in Schedule 2 had been met. In the case of "sensitive personal data"(now known as "Special Categories") any one or more of a series of conditions in Schedule 3 had to be met.

Once again, we will set out the DPA 1998, and highlight how this has been changed by the GDPR ***<u>and DPA 2018</u>***. ***<u>These are "exceptions" i.e. you can process personal data if one or more of the following applies.</u>***

The conditions in Schedule 2 are that processing is necessary:

(i) Because the data subject has given his consent (**for one or more specific purposes)**

(ii) For contractual performance (or taking steps to enter into a contract, requested by the data subject)

(iii) Because the data controller is required to comply with a **[**(non-contractual)**]** legal obligation

(iv) To protect the vital interests of the data subject **[or another natural person]**

(v) (loosely) to carry out any statutory or other function of a public nature imposed on any person **(processing is necessary for the performance of a**

task carried out in the public interest or in the exercise of official authority vested in the controller – almost the same but not quite)

(vi) Processing is necessary for the legitimate interests of the data controller or any third party to whom the data are disclosed unless the data subject's rights and freedoms are prejudiced **(particularly where the data subject is a child).**

The DPA 2018 has something to say about point (v) above. It says (s.8) that this "includes" – and is presumably therefore "not limited to"- (a) the administration of justice, (b) the exercise of a function of either House of Parliament, (c) the exercise of a function conferred on a person by an Act or rule of law, (d) the exercise of a function of the Crown, a Government Minister or a government department, (e) an activity that supports or promotes "democratic engagement" – whatever you conceive that to be, as it appears not to be defined.

The conditions in Schedule 3 of the DPA 1998 are that processing is necessary:

(1) Where the data subject has given explicit consent **for one or more purposes (unless the law prevents the prohibition being lifted by the data subject)**;

(2) For carrying out any right or obligation imposed on the data controller **or data subject** by law **or a collective agreement providing for safeguards for the rights and interests of the data subject** in connection with employment **and social security and social protection law**;

(3) In order to protect the vital interests of a data subject where the latter cannot give consent or the data controller cannot be expected to get consent; (**where the data subject is physically or legally incapable of giving consent);**

(4) For a non-profitmaking body, which exists for political, philosophical, trade union or religious purposes, and the processing relates only to members of that body or have regular contract with it, and is carried out with appropriate safeguards for the rights and freedoms of the data subject and the data is not passed onto a third party without the data subjects' consent;

(5) The information in the personal data has been **manifestly** made public **(**deliberately) by the data subject;

(6) For actual or potential legal proceedings or obtaining legal advice or otherwise defending legal rights **or for the establishment, exercise or defence**

of legal claims or whenever courts are acting in their judicial capacity [*Note that this exception will be widened by Schedule 1 of the Data Protection Bill currently before Parliament, but the text has not yet been finalised…***…….but has now - see DPA 2018 below!)**;

(7) (loosely) to carry out any statutory or other function of a public nature imposed on any person; **(for substantial public interest based on the law, subject to data subject safeguards) [***The Data Protection Bill will in some ways limit this ground- see below for the DPA 2018]*

(8) **[**For anti-fraud purposes**];**

(9) For medical purposes (preventative **or occupational** medicine, **for the assessment of the working capacity of an employee** medical diagnosis, medical research, the provision of **health or social** care **[**and**] or** treatment **[**and**] or** the management of health **or social** care **systems [**services**]**) by a health professional or equivalent, **or pursuant to law.**

(10) **For public health reasons (e.g. cross border health threats, quality of medicinal products or medical devices) subject to the rights and freedoms of the data subject;**

(11) **Archiving purposes in the public interest, scientific or historical research or statistical purposes;**

(12) **[**For the promotion or maintenance of racial or ethnic equal opportunities, where information about racial or ethnic origin is involved.**]**

Once again, the GDPR changes (see Art.6 and 9) have been overlaid in bold text.

Personal data relating to criminal convictions is now dealt with separately from other Special Categories (***see heading below for words about criminal convictions)***. The GDPR contains a very wide prohibition on processing this personal data. But there will be an exception in the new Data Protection Act (***DPA 2018)*** to cover processing in connection with legal proceedings and legal advice.

So what does the DPA 2018 actually have to say? We are back to Schedules again! Fasten your seatbelts for some convoluted drafting.

Mostly, the DPA 2018 is about giving some substance to "Special Categories" personal data (Article 9) and criminal convictions data (Article 10).

Firstly, if you are relying on points (2), (9), (10), (11) above to process data, one of the following conditions has to be met (under the DPA2018 Schedule 1 Part 1):

For point (2), the processing of personal data has to be in respect of a legal obligation/legal right imposed or conferred on the data controller/data subject concerning employment, social security or social protection, and the data controller has to have an appropriate policy document in place to cover this. Details of what is required by the latter are in Schedule 1 Part 4 para 39.

For point (9), Schedule 1 Part 1 para 2 sets out what exactly are the "health and social care purposes" which allow the controller to process personal data e.g. medical diagnosis. There is also a reminder to the data controller to take into account secrecy obligations (see GDPR Art.9(3)) and confidentiality responsibilities (see s.11(1)).

For point (10), the condition is met if the processing of personal data is necessary for public interest reasons in the area of public health and is carried out by a health professional or another person who is required by law to abide by confidentiality provisions.

For point (11), personal data can only be processed if this is necessary for the defined purposes, the safeguards in GDPR 89(1) and DPA 2018 s.19 are implemented and the public interest is served.

Secondly, In respect of point (7) – and yes, there is a reason for taking these out of order; it is covered by DPA 2018 s.10(3), the others above fall under s.10(2) - "public interest" processing is only allowed if the conditions in Schedule 1 Part 2 are met.

This is a long Schedule with a number of different "public interest" activities in it. The baselines, however, are that (a) any data controller has to have an appropriate policy document in place - see above Schedule 1 Part 4 para 39, and (b) there is substantial "public interest" in what is being processed.

How might the Bar be affected? In amongst the various "public interest" activities, you may wish to look at:

- *para 6 (you have to process personal data because a statute/rule of law requires you to do so)*
- *para 7 (the administration of justice)*
- *para 12 (processing of personal data in order to help determine whether someone has acted unlawfully with respect to a regulatory requirement – but, in this case is dependent upon you not being able to get the data*

subject's consent to processing and in many cases, the Bar will have obtained that consent.)

- ***para 18 (safeguarding of children and others at risk – family and mental health lawyers please note)***
- ***para 19 (safeguarding the economic well-being of individuals -again, family lawyers please note)***
- ***para 21 (advising on occupational scheme entitlements/eligibility and the data concerns the health of certain relatives – pension lawyers please read.)***
- ***para 26 (you can process "special categories" data for the purposes of publishing a court judgment/tribunal decision - those in part-time judicial positions and those involved in law reporting please note)***
- ***para 28 (measures designed to protect standards of behaviour in sport – sports lawyers may want to read this one).***

Criminal convictions

The DPA 2018 s.10(4) addresses the processing of personal data relating to "criminal convictions and offences or related security measures" that is NOT carried out by official authority. This is one area where the UK has been allowed to implement its own specific measures under Art.10 GDPR. Any processing of personal data meets the requirement of this Article ONLY if it meets a condition set out in Parts 1,2 or 3 of DPA 2018 Schedule 1.

We have dealt with Parts 1 and 2 above. Part 3 contains additional conditions under which processing of data relating to criminal activity may be permitted. So, you can process personal data if one of the following conditions is met. These include:

- ***Consent – if the data subject consents to you processing the data (para 29)***
- ***Protection of an individual's vital interests and the data subject cannot physically or legally give consent (para 30)***
- ***Published personal data – you can process data which has manifestly been made public by the data subject (para 32)***

- ***Legal activities – you can process personal data if it is necessary:***

  (a) for the purpose of, or in connection with actual or potential legal proceedings

  (b) for the purpose of obtaining legal advice

  (c) for establishing, exercising or defending legal rights (para 33)

- ***Judicial activity – you can process personal data relating to criminal convictions etc. if you are sitting as a judge (para 34)***

- ***A Schedule 1 Part 2 condition is met but without the requirement for the public interest element (para 36).***

Criminal lawyers may also want to glance at para 35 concerning the administration of accounts for payment cards used in the commission of indecency offences involving children.

We are not finished yet! There is a new Art. 7 "Conditions for Consent", which contains stricter requirements for obtaining the consent of data subjects (i.e. GDPR Article 6.1(a)). However, consent of the data subject cannot safely be relied on in all situations. Consent might be withdrawn, and it will usually not be possible to obtain consent from persons other than your client, for example from witnesses who are expected to be called by the other side. To cover these situations, you will need to rely on one of the other grounds:

- For ordinary personal data you will usually be able to rely on the "legitimate interests" ground, (vi) above. For this you need to have identified the legitimate interest which you are relying on (e.g. provision of legal advice, complaints handling, fee disputes, pupil training, conflict checks), and you should identify this interest in your notification to data subjects and in your data protection policy.

- For Special Categories of personal data and data about criminal convictions you will need to rely on the "legal claims" ground, or one of the one of the grounds to be contained in the new Data Protection Act.

The stricter requirements for consent:

- If you are relying on "consent" it has to be informed consent;

- Informed consent means clear and affirmative action by your lay client (see ICO Guidance at ***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/.*** ***For those diligent souls who have noticed this reference is different from the first version of this blog, this is because the guidance has been superseded.***

- "Clear and affirmative" means putting appropriate words into your privacy statement and in your contractual terms.

- If you do put words into your contractual document, these have to be clearly distinguishable from other matters; make them prominent and probably put them at the beginning of your contractual terms so they are the first thing a client reads or at the end and requiring an additional confirmation.

- Make sure the contract is signed. If you are contracting with a solicitors' firm, you will need a separate data protection consent from the lay client.

- **You** have the burden of demonstrating that that your client has given his/her consent to processing.

- Make it clear in any document what happens if the client declines to give consent – ***you can't do the work.***

- Any statement concerning data protection has to be intelligible, using clear and plain language.

- You cannot rely on a pre-ticked check box to establish consent.

- Statements like "if you don't wish to consent to me processing your personal information, you may opt out by informing me in writing" are not acceptable.

- A consent statement also has to be easily accessible – it is no good referring to "our data protection statement which is available on request".

- Note that a client has the right to withdraw his/her consent at any time (e.g. withdrawal of instructions). You need to tell him/her that this is the case before he signs up. Put this in your contractual terms/data protection notice issued to the lay client.

- You are safe as regards what you may have processed up to the point of withdrawal of instructions. What do you do afterwards (e.g. processing for conflicts, fee disputes, potential complaints)? You probably have to rely on (ii), (iii) or (vi) above to justify processing.

- You cannot rely on express consent if the nature of your instructions changes. You have got to seek it again in the context of the new role you are undertaking.

- Look again at the Principles as a whole. If the client withdraws instructions, does anything else have to be done? For example, you should not hold onto his/her data for longer than is necessary.

Conclusion

We have (a) summarised the basic Principles with which a data controller has to comply (b) traced the changes from the DPA 1998 to the GDPR ***to the DPA 2018*** (c) looked at Principle 1 - "lawfulness, fairness and transparency" and addressed the difficulty in relying on consent and the methods of obtaining consent effectively. In the next Chapter, we will look at "fairness" and "transparency".

Bar Council IT Panel