GDPR Blog Chapter 10: Epilogue – *updated for the Data Protection Act 2018*

Well folks, all good things have to come to an end. Over the last ten or so issues of Bar Talk, we have dissected the General Data Protection Regulation (GDPR) to try to simplify the subject of data protection and the issues that arise from it. There is an Introduction and a series of "Chapters", adopting the very obviously appropriate metaphor for the Bar, of the scenes of a play.

This is Chapter 10, the last Chapter in this series. We hope you found the previous Chapters useful, and, of course, we are certain you will have found them an absolute joy to read!

We have broken down the new Regulation into a number of theatrical scenes, dubbed Chapters. This seemed to us to be an appropriate metaphor for the Bar. So far, the scenes are as follows: 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 (Roles of the principal members of the Cast – the Data Processor *[here]*, and Chapter 7 (The Melodrama Part 1 -What happens when it all goes wrong) [here]; Chapter 8 (the Melodrama Part 2 – How much could it cost you to get it wrong) *[here]*, and Chapter 9 (International Transfers of Data) [here].

Now it is time for the Epilogue; a summary of the scenes played out over the last nine Bar Talks. The intention is to home in on some of the most important requirements that you need to understand and adopt to comply with the GDPR. We will do this by a series of questions and answers, with references to the relevant Chapters where you will obtain more detailed information (numbers in brackets).

What role do I play?

As a practising barrister, you will be a "Data Controller" (2,3,4) for data protection purposes. You will almost certainly be handling ("processing" in the GDPR jargon) personal information ("Personal Data" in GDPR speak (1)) about individuals ("Data Subjects") on a daily basis. It is you who decides the purposes for which the Personal Data are to be used and how this is achieved. Hence you are a "controller" of that Personal Data.

"Processing" has a very wide ambit indeed (1) and covers just about everything you can do electronically. You should remember that processing Personal Data in hard copy files is also covered (1), provided that the file is structured in such a way that these can be obtained easily from the files.

While we are familiar with the idea that our case files are confidential, some Personal Data is super-sensitive ("Special Categories" in GDPR terms) and you need to handle that with particular care. This includes such matters as physical and mental health – see (1) for the others.

Do I have any other part to play or responsibility to exercise?

You may also be a "Data Processor" (1)(6). For example, your Chambers may ask you to handle recruitment of a new staff member, pupil or tenant. Chambers is the Data Controller; you are processing Personal Data about applicants on Chambers' behalf. Please see those two Chapters which set out the position on Data Processors.

Also, remember that you personally may be engaging Data Processors. These may be internal: Chambers' staff, full-time pupils, mini pupils and work experience pupils. They will be your Data Processors but you are responsible for their compliance with data protection law. Your Chambers' Data Protection Policy should cover the issue of Bringing Your Own Device, where a pupil uses his own computer to do your work. Ensure they don't let the cat out of the privacy bag!

Secondly, you may want to recruit external Data Processors. The most obvious are organisations which will store your data for you, known as "cloud service providers". Ensure that they have their storage devices located within the EU or another location with acceptable data processing standards (see (9) for the reasons).

In all cases the obligations of Data Processors must be set out in a contract (see 6). This includes Chambers (or the Head of Chambers) , barristers when acting as Data Processors, devils, pupils, mini-pupils, IT consultants, email service providers, cloud storage providers, and other service providers.

Do I have to register with anyone to process Personal Data?

Under the old UK Data Protection Act (DPA), yes. And you had to declare the (very) general purposes for which you processed Personal Data. The Bar had a standard purposes template. Under the new GDPR regime, the primary emphasis is on telling Data Subjects who you are and what you are about, rather than registration with a central authority. So much for the good news. The bad news is that it is likely that

there will still be a fee for processing data and that for some, it will increase from its present £35 to £55 (assuming you pay by direct debit). If Chambers is turning over more than £36M or has more than 250 staff then it goes up to £2895 (on the same assumption).

What general obligations should I be aware of?

You have to process Personal Data in line with a number of Principles. These have been in place since the DPA came into force but have been expanded or restated in the GDPR under Article 5. We will not repeat them in detail here but simply refer you to them in (2)(3)(4).

What is far more important is how you should now act in your daily practising lives. A non-exclusive list includes:

(a) You are required to be "accountable" for your Personal Data processing i.e. if called upon you have to demonstrate that you have complied with the data protection Principles (2). Under the DPA you merely had to comply.

(b) You and your Chambers should now have a Data Protection Policy.. Please read it and adhere to its provisions. If there is any ICO investigation it will help to persuade the ICO that this new and more onerous data protection regime is being taken seriously.

(c) This policy should set out retention periods for Personal Data i.e. how long do Chambers and Chambers' members intend to keep Personal Data. There is no fixed answer to this; it depends on which legal areas comprise Chambers' members' practice. If there are a number of different practice areas, different periods of retention may legitimately be chosen. If an individual decides to deviate from a standard Chambers' policy, this should be recorded and for ease of reference a copy should be kept by Chambers as well as by the individual together with the general Chambers policy. You may find it easier simply to place a privacy notice on your page of your Chambers website. In all cases, the reasons for choosing a particular period should be stated.

(d) Adopt a new way of thinking. Get rid of all your unwanted **hard copy** files; purge your computer of those thousands of **old emails** that you have hoarded in case they might be useful. Remove all of your **old cases** from your PC. If you want to keep precedents like pleadings, orders and opinions, then you can, but you have to anonymise them by removing the Personal Data– try

Find and Replace on Microsoft Word (and its equivalent for other programs). If they are in PDF format, you will have to redact the Personal Data or convert them into Word format and then dispose of the PDF. It's a good idea to store these separately in a new folder called e.g. Precedents. Oh, and don't keep **new cases** on your PC longer than is strictly necessary. The next paragraph details the possible legitimate grounds for keeping files at least until about a year after the end of the limitation period. You may wish to move closed cases to a secure (offline) archive ready to be deleted when the time comes.

The only reasons to keep files after the case is finished will usually be the following legitimate interests (i) handling possible complaints, (ii) payment issues, (iii) regulatory reasons, e.g. money laundering, (iv) appeals (although for civil cases this will usually be known before a case is considered 'closed'), (v) the Personal Data is needed for a related case, (vi) conflict checks; however, that limited subset of data can be kept on the Chambers' system - it's usually the clerks that check, after all. The 'legitimate interests' basis does not apply to Personal Data in the Special Categories, retention of which data beyond a reasonable period after the expiry of the limitation period requires explicit consent, and if the retention of the data is otherwise particularly damaging to an individual you may have to undertake an individual assessment of the justification for retention.

(e) If you wish to retain some documents for a specified purpose – then you will need to think carefully about the legitimate basis for why you are keeping them and whether you can justify retaining them with all the Personal Data and still comply with the requirement for data minimisation. It is difficult to see how you could do this but if you think you have a justifiable reason make sure that the reason and justification is recorded.

(f) Compliance with (c) and (d) will mean you have complied with several important data protection Principles without really thinking too hard about them. You will have kept Personal Data to a minimum by deleting it or anonymising it and by keeping a record of your decisions you are accountable for the decision, and the reasons for the processing are transparent.

(g) For the future, store emails and files in a way which will make it easier for you to delete them when the time for deletion arrives. Best practice is to create separate sub-folders for each case and a separate set of folders for old cases and precedents.

(h) Turn your PC into Fort Knox – impossible to get into, should you accidentally leave it on the train. That means (i) use a strong password and encrypt all mobile devices including laptops (your laptop should already be encrypted but if not and you are running Windows 10, try Bit Locker which you will conveniently find on your PC). The password does not have to be the usual "upper case-lower case-numbers-unusual symbol" formula which you will promptly forget. Unusual but easily recalled wording will do e.g. "dog-likes-bones", (ii) keep a separate email account for professional Bar activity – you can then delete professional emails but leave personal ones, (iii) consider encrypting the data on your desktop PC – then nobody can read it, (iv) ensure you have anti-virus software loaded and keep it updated, (v) keep your firewall turned on, (vi) implement all operating system updates and upgrades that are offered, particularly if they refer to implementing security protection.

(i) Exercise caution. Someone, somewhere may send you an innocent-looking email which will not be captured by anti-virus software. It might be a purported invoice or a request to update a computer program you run or reply to a survey or a purported message from your bank or a solicitor or colleague asking you to look at correspondence, and it may appear to have been sent to you by one of your contacts. <u>If it does not look right, don't open any attachment or click on any link in the email</u>. If you have an IT manager, send it to him/her for verification, or open it on a device which does not matter (e.g. a personal smartphone which is not linked to Chambers).

(j) Record keeping; a good idea in any event for all the decisions you make about your policies. More will probably not be generally required unless there are more than 250 employees. However, if you are processing "Special Categories" data or criminal convictions/offences you are required to keep specific records (see Arts. 9 and 10). Details of what is required are in Art.30.

How should I behave towards solicitors, clients and others?

(a) So much for internal organisational matters. Now, how do you deal with lay and professional clients and others? The most basic and important Principle (the 1st Principle in the DPA and in GDPR Art.5) is that as a Data Controller, you are required to process Personal Data "*lawfully, fairly and transparently*" - known as the "Lawfulness Principle" (2).

At its most basic, this means ensuring that you have a lawful basis, or permission, for processing Personal Data. The DPA provided that such permission could be assumed in a number of circumstances – see DPA Schedule 2, and Schedule 3 where "sensitive data", (now known as "Special Categories" data) was concerned (2).

Most obviously, this arises where the individual has given specific consent to use his/her Personal Data ("actual and informed consent") – Art. 6(1)(a) We dealt extensively with how you should handle this aspect in (2). Please re-read this.

(b) However, explicit consent is **not** required (and may be hard to get if the Data Subject is someone other than your client) if your processing falls under one of the other provisions i.e. Arts 6(1) (b) – (f).

For example:

(i)You need to process Personal Data for the purposes of "legitimate interests" you are pursuing. As a barrister, your "legitimate interests" will be to provide legal advice and assistance to your client.

(ii) You are processing Special Categories data, for the "establishment, exercise or defence" of legal claims.

(c)The other main part of the Lawfulness Principle is that you have to act "transparently". This is not rocket science. It simply means you have to be open about who you are and what you are doing. Subject to some important exceptions, you must promptly notify Data Subjects, including third parties such as witnesses on the other side, that you are processing their Personal Data and provide a long list of associated information. But you **don't** need to notify them if you are legally obliged to keep the Personal Data confidential (e.g. because of the Bar Code of Conduct), it is privileged or if the provision of the information about your processing is impossible or would involve a disproportionate effort -or quite simply, if they already have all this information – unlikely but possible.

(d) A lot of detail has to be provided to Data Subjects (3) under the "transparency" obligation. The GDPR breaks this down into two responsibilities (i) information to be provided to the Data Subject, assuming the Personal Data is obtained from that person (ii) information to be provided to the Data Subject if the Personal Data has NOT been obtained from that Data Subject (see Arts. 13 and 14). It is likely that the detail will be presented as standard information with you filling in gaps e.g. in order to provide legal services to clients, to deal with complaints, for regulatory purposes (such as money-laundering records), and so forth.

(e) A word about the reasons you are holding someone's Personal Data. The Purpose Limitation Principle (DPA Principle 2 and GDPR second principle in Art. 5) requires such data to be held for specified, explicit and legitimate reasons. As we have said, you no longer register with the ICO in general terms; you account for what you are doing in specific terms. Watch out! You cannot simply invent more purposes that go beyond the purposes which you have set out in your notifications to Data Subjects.

I have complied with all the Principles; do Data Subjects still have any recourse to me?

Getting all your data protection ducks in a row is not the end of the story. Chapter 5 looks at the rights of Data Subjects. We refer you back to this Chapter in the event that a Data Subject approaches you with a request about his or her Personal Data. You have a limited time in which to respond to these requests – one month, down from the original 40 days.

In summary, this could include a request:

(a) to know whether you are processing his or her Personal Data, and if so what;
(b) to rectify inaccurate Personal Data or, complete it if it is incomplete;
(c) to be "forgotten" – this applies only in certain circumstances (see 5);
(d) to restrict processing e.g. if a Data Subject makes an allegation that Personal Data is inaccurate;
(e) to object to continued processing;
(f) for all Personal Data to be ported to another Data Controller.

We mention these in the context of a roundup of the various issues that may come to affect you. Please look at (5) if you want more detail.

I have made a fool of myself……..I have lost my computer…….what now?

You are off to a head start if you have already implemented the security measures we have suggested above. But apart from those comfort factors, you may have obligations to tell different people what has happened.

You are obliged to tell:

- the ICO, unless the individuals in your data are unlikely to be seriously compromised
- Data Subjects, where there is a high risk that their rights and freedoms are put at risk
- your Data Controller, if you are a Data Processor.

You may also need to tell:

- your Chambers (partly so that they can assist you, partly because this should be part of their Data Protection Policy and partly so that any remedial steps can be taken)
- the BSB – if a loss might be considered as serious misconduct
- the police/insurers.

Please look at (7). In the case of the ICO there are very short time limits within which you have to report a loss of Personal Data, however this arises. Worse, you may have to provide information about the loss to the ICO. Most barristers have very busy lives; reporting to the ICO is a serious distraction. Reporting a data loss to your clients or Data Subjects is something you really want to avoid – as we said in the Introduction *[here]*, how embarrassing is that? You can avoid doing this – but look at (7) to see how!

You or your Chambers should have in place a Data Breach Response Plan so that you are ready to take the necessary steps promptly in the event of a data breach occurring. There is one set out in the Riliance pack which is available free to barristers who register at https://riliance.co.uk/barristers-gdpr#overlay-context=barristers-gdpr

Finally, the Bar Council has a detailed guidance document on Data Security and what steps to take if the worst happens *[here]*.

What can the ICO do to me if I do lose all my data?

Please have a look at (8). We won't rub your noses in it but there are potentially some fairly massive fines that the ICO can levy. And they have all sorts of investigative and corrective powers. This is not however an on-the-spot fine. The ICO will investigate what has happened and take all relevant factors into account. Look at Art. 83 GDPR – a lot of the measures we have suggested you take, will count in your favour if you have implemented them, and will, correspondingly, reduce the level of any fine.

I do a lot of cross border work…..what risks should I be aware of?

Remember: it is "Personal Data" that is the worry. There are strict limitations on the transfer of Personal Data to third countries which you must comply with. If you are working across borders in the EU areas, there will be no concern, as each Member

State has to abide by EU data protection standards. The European Commission approves other countries against a series of criteria and details are on the EU website. Some organisations in the US currently operate under an EU-USA Privacy Shield for companies that sign up to this (please check the list of companies). However, there is no guarantee that a foreign government will not want to see the data especially if you are involved in high profile extradition proceedings. Please be aware of the risks to your clients. For transfers to other countries, transfers will only be possible if you have referred to the intention to transfer to that country in your notification to the Data Subject, and you either have the consent of the Data Subject or the transfer of personal data is necessary for the establishment, exercise or defence of legal claims, or one of the other derogations applies. Chapter 9 will assist you.

Conclusion

That is all from us at the moment. We hope it has been useful. If you have any questions on any aspect of what we have written, please look at the Ethics Hub first – there is much more specific guidance there. If that doesn't answer your question, address it to the IT Panel and we will endeavour to answer it. Who knows, perhaps we will receive so many questions that more blogs will be justified!

Bar Council IT Panel