IT Panel Blog – The Data Controller – principles cont.

Welcome to Chapter 4. For those who have missed the action so far, there is a new Data Protection Law arriving at a theatre near you in May 2018. It will be billed as the new Data Protection Act (***DPA 2018)*** and the much-loved and often-reviewed Data Protection Act 1998 ("DPA 1998") will be no more.

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- the Data Controller) [here]. Chapter 3 finished off the data controller's role with regards to Principle 1 [here].

Please take a few minutes to cast your eyes over what we have said so far.

Chapter 4 looks at the remainder of the Principles with which the Data Controller - definitely you, as a barrister, and almost certainly your chambers - have to comply with when handling information about a living individual, known as "**personal data**" in the data protection trade.

Principle 1 requires you to process personal data "lawfully, fairly and in a transparent manner". As we have said, we have discussed this in earlier Chapters. We will now briefly discuss the other Principles.

Principle 2 - Purpose Limitation (GDPR Art 5.1(b))

When you handle someone's personal data, it has to be for "specified, explicit and legitimate purposes".

Under DPA 1998, you had to register these purposes (which were expressed in general terms), pay a fee and go on a public register. The Guidance [here]suggests this may be a thing of the past.

[Note: although registration may no longer be required, that does not mean that you will not have to pay for the privilege of processing personal data. Under proposals made last year there would be, as now, different levels of fees depending on factors such as the size of the processor and the amount of processing. In that proposal, the fees for barristers and Chambers would increase from £35 to £55 per controller per annum.]

DPA 2018 makes provision for data controllers to pay charges to the ICO (s.137, Schedule 20 para 26 which expressly continues The Data Protection (Charges and Information) Regulations 2018 SI 2018/480) - see [Bar Council Data Protection Fee guidance here], and https://ico.org.uk/for-organisations/data-protection-fee/ for the ICO's guidance in relation to the fee. Please note: S.137(2) provides that data controllers may be required to pay a charge whether or not the Information Commissioner has provided, or proposes to provide, a service to the data controller.

In any event, you will still be subject to the Principles**. The notification will now be to data subjects, such as your client.**

What this means for the Bar and Chambers

- You have to provide information to data subjects about what you are processing and why
- This is likely to resolve itself into a series of standard terms to be used appropriately and which will reflect the existing notifications to the ICO, but with some additional content
- Communication is everything. Have a look at Chapter 3 under Transparency for the form of notification [here]
- "Legitimacy" comes under Principle 1 - have a look at Chapter 2 "Lawfulness" for what this means [here]
- If you provide information to the data subject about what you are processing and the purposes for which you are processing it, you cannot then further process that information for other incompatible purposes.

Principle 3 and Principle 5 - Data Minimisation and Storage Limitation (Arts. 1(c) and 1(e) and 25)

A quick reminder: "Data Minimisation" means that any personal data obtained by you has to be "adequate, relevant and limited" for the purposes for which you intend to process it. "Storage Limitation" means you cannot keep data for longer than necessary for your intended purposes - at least not in a form that permits identification of the particular data subject.

These might usefully be referred to as the "spring cleaning" principles; making sure things are tidy to start with and then clearing out what you really don't need at the end. They naturally go together.

The whole aim of the game is to cut down the amount of personal data that you are either actively using or storing (unless in the latter case, you go to the trouble of anonymising the data). This ensures that clients and others are not exposed to the possibility of their data becoming generally available when this could have been avoided.

Art.25 is not the easiest provision in the world to understand. The heading is "data protection by design and by default". We will try to unpick its provisions.

1. By Design (Art.25(1)) Basically, when you are processing personal data, you are required to have designed in and actually implement effective measures to protect a data subject's rights and to meet the requirements set out in the Regulation. A chambers IT manager may be able to advise on suitable processes to be implemented. These should be set out in a chambers' IT Guide.

2. These measures could be technical (e.g. using impossible-to-guess passwords, data encryption) or organisational or both; it does not matter.

3. Suggested measures include "pseudonymisation" and "minimisation". The former renders the data effectively anonymous (e.g. a name is replaced with a letter). It is hard to see why the Bar should be doing this, but in direct access cases you may have to. The latter suggests that you don't keep everything forever, and you don't keep anything for longer than is necessary. Everyone does and now it has to stop. We used to return hard copy files to solicitors at the end of a case to avoid cluttering up our rooms with paper. Now we have to remove softcopy files - but perhaps to a chambers management system where they can be encrypted and put out of harm's way until the point in time is reached when they need to be deleted altogether. They can be kept there or in another secure archive facility against the need e.g. if a client complaint arises.

4. There is a little bit of a let out. The Article allows you to take account of "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing" as well as the "risks of varying likelihood and severity" for data subjects posed by the processing you are undertaking.

5. By default (Art 25(2)). This part requires you to ensure that by default only personal data which are necessary for each specific purpose of the processing, are processed. "By default, "means that you have to have procedures in place which ensure that data is minimised appropriately without you having to take positive steps each time to achieve this, including a procedure for deleting data when the retention date for that data (see below) has been reached.

6. Since "processing" has a wide definition, paragraph 5 (above) therefore points to the amount of data collected, the extent to which these are processed, the period they are stored and how accessible they are. There is a particular emphasis on ensuring (by default, of course), that data is not made accessible to large numbers of people without your intervention. You are required to take whatever "technical and organisational measures" as are appropriate to meet this requirement.

What does this mean for the Bar and Chambers?

We would suggest the following:

- You have to adopt a different mindset once this Regulation ***and DPA 2018*** come into force. Your solicitors will have to do so as well. Decluttering is the new watchword!

- As soon as possible your chambers needs to prepare a policy for deleting and retaining data which will be appropriate for most of the work carried out by members of chambers. It will need to be flexible enough to cater for individual barristers to vary it to reflect the requirements of their individual practices (e.g. cases involving children may require retention for a longer period, until after the children are 18 years old). This should set out how long you intend to keep personal data - oh,

and remember that under Art.13, you have to tell the client how long you intend to keep their data when instructions are accepted. This should reflect your data retention policy or if you need for any reason to exceed time limits in this, then the client needs to be informed.

- You will then need to look at your Chambers policy and consider whether you personally need to make changes or additions. If you decide that you need variations, you will need to record your own policy, and keep it somewhere where you can find it in the event of a complaint. Probably best if you log it alongside the Chambers' policy.
- After you have decided on your policy, you will need to spring clean your computer(s) and backup devices. If you are storing old casefiles (i.e. the case is finished) electronically, then delete everything which, applying your policy, you no longer need to keep. For what remains, either move the data to your chambers' central storage or alternative secure offline storage or ensure that the data is encrypted or take the time to ensure that the personal data in the files is rendered anonymous. (Note: moving the data to a secure encrypted offline storage and locking the device away somewhere safe does not amount to deletion of the data. You will obviously still need to keep your data backed up for some purposes, but your backups should contain only the data which, according to your policy, you have decided needs to be kept.)
- If you are storing old hardcopy files, then extract what you need from these (probably your opinions and pleadings) and return the rest to your solicitors (or, with their permission, send the files to the secure shredder). You can always redact specific personal data before filing these (physically or by scanning).
- For old emails, (needed for conflict checks, use as precedents etc.) move the likely sources of personal data - email attachments comprising instructions, witness statements, correspondence etc. to the case files and then treat these as set out above.
- Consider whether separate email accounts are now in order for your private and professional purposes. You can then delete professional emails, whilst always retaining your personal ones. It will be much easier to delete data you no longer require if you keep emails for each case in a folder for the year and a separate sub-folder for each case below that.
- For current files and emails, you will almost certainly need to keep personal data for at least a year after the maximum relevant limitation period from a defined endpoint. What is an endpoint? This could be (for example): the end of all possible appeals; the date you received your last fee; the date you wrote off the fees.
- For Direct Access/ Transactional Advisory Work. You need to keep records for money laundering checks - these should be kept for 5 years (a) from the data the business relationship ends (b) the date the transaction is completed.

- There are a whole lot of practical steps that you can take to assess what you have and how this should be handled in the main Guidance [here] - see pages 30-31.

We understand that you might consider all this to be a burden too far in already busy lives. There are some real practical reasons that may persuade you to adopt a new way of thinking and dispose of old material.

These are:

- This reduces the impact of a data breach resulting from opening a scamming email
- Retention of excessive data might count against you in an ICO investigation
- If there is a data breach, there are less data subjects to notify and less chance that you may have to go public announcing the data breach
- Smaller amounts of data mean it is easier to finds specific data in response to a subject access request
- Data storage space is reduced so computer systems operate more efficiently
- Data held for long periods is likely to become more inaccurate as time goes on resulting in requests to correct or delete it

Planned enhancements to chambers practice management system will also assist you.

Principle 4 - Accuracy (Arts.16,18,19)

We will deal with this in a later Chapter under the rights of data subjects to have their personal information corrected.

Principle 6 - Integrity and Confidentiality (Arts.24, 28,29 and 32)

Article 24 - we dealt with this in Chapter 2 as part of the Data Controller's responsibilities.

Articles 28 and 29 - this concerns the responsibilities of the Data Processor under this general heading. We deal with this in a later Chapter.

Article 32 - This deals with security of processing. It applies to both data controllers and data processors. There is existing Guidance from the IT Panel on this issue based on DPA 1998 [here].

What does it say? Essentially, use appropriate security measures having regard to what you are doing, the likely risks to data subjects, the implementation costs of security measures, and the current technical state of the art. Security measures can be both technical and organisational.

What does it suggest? The Regulation lists a number of non-exclusive pointers to help you achieve this. These are:

- Encrypt all personal data in your possession
- Where possible, anonymise that data
- Adopt appropriate confidentiality measures and ensure the integrity, availability and resilience of your processing systems and services
- Adopt appropriate disaster-recovery and back-up systems
- Regularly stress test the systems you have in place for their security effectiveness
- Consider the risks you particularly have to take into account. These are: accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

What does this mean in practice? You, and where appropriate, your chambers should adopt the following measures to maximise your protection.

- Computers should have strong passwords
- Ensure that the password you use is used only for this purpose and not on websites that you use e.g. for shopping or gaming
- Anonymise data where practicable to do so (e.g. a name becomes a number)
- Using encryption software which scrambles words - use it on everything; phones, USBs tablets, laptops, and consider desktops too
- Dispose of old hard disk drives securely (use a recognised security company and obtain a certificate of destruction or literally destroy them. Don't just send data to the "Dustbin" icon; data can still be retrieved)
- Apply all operating system updates - these should be automatically downloaded
- Don't use an unsupported, out of date operating system - if you are it is probably time to change your computer
- Employ anti-virus software and keep it updated. Chambers may install this for you. Check if they do.
- Ensure your pupils know about policies and procedures for Bring Your Own Device (BYOD). There is Bar Council Guidance on this [here].Remember they will be processing personal data provided by you when they write that opinion for you. Make sure this is deleted from their computers when they leave chambers
- Consider using encrypted email for "Special Categories" of data (formerly known as "sensitive data")
- Consider using encrypted email for sending links to cloud storage - there is Guidance [here]

- Back up your data. Most chambers will have back-up systems but if you want to use your own, keep any device well away from the Internet where it could be attacked by viruses - if you leave it plugged in to your computer your data is at risk from some forms of attack.
- Don't open attachments on emails if you are unsure of the email's origin. Some are clever; they purport to come from your bank or Microsoft or your solicitor or ask you to verify an invoice -be careful. These could contain viruses (whose aim is random destruction) or "ransomware" (whose aim is to extort money). If you have a feeling something is not right, DON'T OPEN IT! Trust your instincts and phone the apparent sender, if your solicitor, or contact your Chambers IT manager for advice on what to do. If you discover a problem, warn the sender and, if possible and appropriate, other members of Chambers.
- For chambers' IT Managers, regularly audit your facilities, equipment and procedures.
- Ensure there is a policy and procedures for dealing with hard copy files (remember: structured manual filing systems are included in the Regulation).

Bar Council IT Panel